

# DEVICE AND METHOD FOR INFORMATION PROCESSING AND STORAGE MEDIUM

**Publication number:** JP2002259605

**Publication date:** 2002-09-13

**Inventor:** IINO YOICHIRO

**Applicant:** SONY CORP

**Classification:**

**- International:** G06F12/14; G06F21/00; G06F21/24; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/00; H04L29/06; H04L29/08; H04N7/167; H04N7/24; G06F12/14; G06F21/00; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/00; H04L29/06; H04L29/08; H04N7/167; H04N7/24; (IPC1-7): G06F17/60; G06F12/14; G09C1/00

**- European:** H04L29/08N5; G06F21/00N7D; G06Q20/00; G06Q30/00A; G11B20/00P; H04L29/06S4; H04L29/06S8D1; H04L29/06S8G; H04L29/06S12A; H04N7/167D; H04N7/24C12P

**Application number:** JP20010050781 20010226

**Priority number(s):** JP20010050781 20010226

**Also published as:**



EP1365536 (A1)



WO02069557 (A1)



US2005262321 (A1)

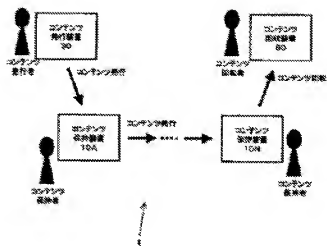
CN1520655 (A)

Report a data error here

## Abstract of JP2002259605

**PROBLEM TO BE SOLVED:** To hold and protect digital information on durable hardware.

**SOLUTION:** A system which moves the digital information without allowing its duplication by using a hardware mechanism generates a record regarding the movement of the digital information, i.e., a transfer history. When the digital information is collected later, what point of time the digital information is copied by altering hardware can be specified by analyzing the transfer history. The data structure of the transfer history is a nesting structure and then while the calculation quantity for transfer history inspection needed for transfer of each time is made constant irrelevantly to the frequency of transfer, tolerance to the alteration of the transfer history by an illegal user in the middle of distribution is also actualized.



Data supplied from the **esp@cenet** database - Worldwide

(51)Int.Cl. <sup>7</sup>	識別番号	F I	アブコード(参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 J 1 0 4
	5 1 2		5 1 2
12/14	3 2 0	12/14	3 2 0 A
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
審査請求 未請求 請求項の数30 ○L (全 28 頁)			

(21)出願番号 特願2001-50781(P2001-50781)

(22)出願日 平成13年2月26日(2001.2.26)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 飯野 陽一郎

東京都品川区北品川6丁目7番35号 ソニ

株式会社内

(74)代理人 100101801

弁理士 山田 英治 (外2名)

Fターム(参考) 5B017 A408 B800 CA18

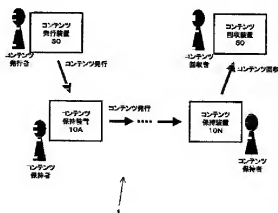
5J104 A409 LA03 LA06

## (54)【発明の名称】 情報処理装置及び方法、並びに記憶媒体

## (57)【要約】

【課題】 耐久性のあるハードウェア上にデジタル情報を保持して保護する。

【解決手段】 ハードウェア機構を用いて複製を許さずデジタル情報を移動させるシステムにおいて、デジタル情報の移動に関する記録すなわち読履歴をとる。後にデジタル情報を回収したときに、読履歴を解析すれば、どの時点でハードウェアの改変によってデジタル情報の複製が行われたかを特定することができる。読履歴のデータ構造を入れ子構造とすることで、各読履歴に必要な読履歴検査のための計算量を読履歴回数によらない一定値としながら、流通途中での不正者による読履歴の改変に対する耐久性をも実現する。



## 【特許請求の範囲】

【請求項1】装置間でコンテンツを交換する情報処理装置であって、

コンテンツ及びコンテンツの読取履歴を送信及び／又は受信する通信手段と、

装置固有の情報を保管する固有情報保持手段と、  
コンテンツを交換する相手側の装置と相互認証する認証手段と、

コンテンツを保持するコンテンツ保持手段と、  
コンテンツの読取履歴を管理する読取履歴管理手段と、  
を具備することを特徴とする情報処理装置。

【請求項2】前記認証手段は、コンテンツを交換する相手側の装置と互いの電子署名の認証を行う、ことを特徴とする請求項1に記載の情報処理装置。

【請求項3】前記通信手段は、前記認証手段により認証に成功した相手側の装置に対してコンテンツを送信する、ことを特徴とする請求項1に記載の情報処理装置。

【請求項4】前記コンテンツ保持手段は、前記通信手段により送信した後のコンテンツを消去する、ことを特徴とする請求項1に記載の情報処理装置。

【請求項5】前記読取履歴管理手段は、  
コンテンツ受信時にはノンスを発生し、

コンテンツ送信時には、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側が発生したノンスTN、並びにコンテンツの読取履歴全体に対する電子署名TSGを含んだ新規レコードをコンテンツの読取履歴に追加する、ことを特徴とする請求項1に記載の情報処理装置。

【請求項6】前記読取履歴管理手段は、コンテンツ受信時に、コンテンツの読取履歴の最後のレコードにコンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、自身が生成したノンスTNが含まれていること、及び／又は、電子署名TSGが正しく読取履歴に対するコンテンツ送信側の装置の署名になっていることを確認することによって、コンテンツの読取履歴を検査し、さらにコンテンツが持つ固有情報がコンテンツ送受信側で一致するか否かを検査する、ことを特徴とする請求項5に記載の情報処理装置。

【請求項7】前記読取履歴管理手段は、コンテンツの読取履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタCAの公開鍵P<sub>ca</sub>を用いて暗号化したもので置換する、ことを特徴とする請求項5に記載の情報処理装置。

【請求項8】前記通信手段は、前記認証手段により認証に成功した相手側の装置から、前記読取履歴管理手段により読取履歴を確認した後にコンテンツを受信する、ことを特徴とする請求項1に記載の情報処理装置。

【請求項9】複数の装置間で読取履歴を作って流通されたコンテンツを回収する情報処理装置であって、  
前記読取履歴は、

コンテンツ固有の情報TIDと、  
コンテンツを読取る度に追加されるレコードと、を含み、

前記情報処理装置は、  
コンテンツ及び読取履歴を受信する通信手段と、  
読取履歴を検査してコンテンツの流通過程における不正を検出する不正検出手段と、を具備することを特徴とする情報処理装置。

【請求項10】前記不正検出手段は、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信したことに応答して、不正の検出を開始する、ことを特徴とする請求項9に記載の情報処理装置。

【請求項11】読取履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置が発生したノンスTN、並びに、コンテンツの読取履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出手段は、読取履歴に含まれる各レコードの電子署名を検証して、整合しない電子署名を有したコンテンツ送信側の装置を不正者として特定する、ことを特徴とする請求項9に記載の情報処理装置。

【請求項12】読取履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置が発生したノンスTN、並びに、コンテンツの読取履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出手段は、読取履歴の先頭レコードに含まれない場合には、該SIDによって識別される装置を不正者として特定する、ことを特徴とする請求項9に記載の情報処理装置。

【請求項13】読取履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置が発生したノンスTN、並びに、コンテンツの読取履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出手段は、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信した場合には、各コンテンツが持つ読取履歴を比較して、同じコンテンツ固有情報TIDを持つコンテンツに付随する読取履歴が正しく先頭のコンテンツ送信側の装置固有情報SIDのレコードから始まり且つ途中で同一内容のレコードを持つが異なり始める枝分かれレコードを探索して、該枝分かれしたレコード中のコンテンツ送信側の装置固有情報SIDによって識別される装置を不正者として特定する、ことを特徴とする請求項9に記載の情報処理装置。

【請求項14】前記不正検出手段は、  
読取履歴の各レコードが所定の管理センタCAの公開鍵P<sub>ca</sub>で暗号化されている場合には、読取履歴に含まれる各レコードを最新のものから順に該管理センタCAの秘

密鍵S<sub>04</sub>によって復号化して検査し、

正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを特徴とする請求項9に記載の情報処理装置。

【請求項15】他の装置にコンテンツを譲渡する情報処理方法であって、  
コンテンツ譲渡側の装置と相互認証するステップと、  
コンテンツの譲渡履歴を更新するステップと、  
コンテンツの譲渡履歴をコンテンツ譲受側の装置に送信するステップと、

前記相互認証並びにコンテンツ譲受側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲受側の装置に送信するステップと、を具備することを特徴とする情報処理方法。

【請求項16】前記のコンテンツの譲渡履歴を更新するステップでは、コンテンツ譲渡側の装置固有情報SID、コンテンツ譲受側の装置固有情報RID、コンテンツ受信側の装置固有情報RID、並びにコンテンツの譲渡履歴全体に対する電子署名TSGを含んだ新規レコードをコンテンツの譲渡履歴に追加する、ことを特徴とする請求項15に記載の情報処理方法。

【請求項17】他の装置からコンテンツを譲受する情報処理方法であって、  
コンテンツ譲渡側の装置と相互認証するステップと、  
コンテンツ譲渡側の装置にノンスTNを送信するステップと、

コンテンツの譲渡側の装置からコンテンツの譲渡履歴を受信するステップと、受信した譲渡履歴を検査するステップと、  
コンテンツ譲渡側の装置からコンテンツを受信するステップと、を具備することを特徴とする情報処理方法。

【請求項18】譲渡履歴の各レコードは、コンテンツ譲渡側の装置固有情報SID、コンテンツ譲受側の装置固有情報RID、コンテンツ譲受側の装置固有情報ノンスTN、並びに、コンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名TSGを含み、  
前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報SID、コンテンツ譲受側の装置固有情報RID、自身が生成したノンスTNが含まれていること、及び又は、電子署名TSGが正しく譲渡履歴に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査し、さらにコンテンツが持つ固有情報がコンテンツ送受信側で一致するか否かを検査する、ことを特徴とする請求項17に記載の情報処理方法。

【請求項19】前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタCAの

公開鍵P<sub>04</sub>を用いて暗号化したもので置換する、ことを特徴とする請求項18に記載の情報処理方法。

【請求項20】複数の装置間で譲渡履歴を伴って流通したコンテンツを回収する情報処理方法であって、

前記譲渡履歴は、  
コンテンツ固有の情報TIDと、  
コンテンツを譲渡する度に追加されるレコードと、  
を含み、  
コンテンツ及び譲渡履歴を受信するステップと、  
譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする情報処理方法。

【請求項21】前記不正検出ステップでは、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信したことに応答して、不正の検出を開始する、ことを特徴とする請求項20に記載の情報処理方法。

【請求項22】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置固有情報ノンスTN、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出ステップでは、譲渡履歴に含まれる各レコードの電子署名を検証して、整合しない電子署名をしたコンテンツ送信側の装置を不正者として特定する、ことを特徴とする請求項20に記載の情報処理方法。

【請求項23】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置固有情報ノンスTN、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出ステップでは、譲渡履歴の先頭レコードに含まれるSIDがコンテンツを発行する所定の装置を示していない場合には、該SIDによって識別される装置を不正者として特定する、ことを特徴とする請求項20に記載の情報処理方法。

【請求項24】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置固有情報ノンスTN、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含み、  
前記不正検出ステップでは、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信した場合には、各コンテンツが持つ譲渡履歴を比較して、同じコンテンツ固有情報TIDを持つコンテンツに付随する譲渡履歴が正しく先頭のコンテンツ送信側の装置固有情報SIDのレコードから始まり且つ途中まで同一内容のレコードを持つが異なり始める枝分かれするレコードを探索し、該枝分かれしたレコード中のコンテンツ送信側の装置固有情報SIDによって識別される装置を不正者として特定する、ことを特徴とする請求項20に記載の情報処理方法。

法。

【請求項25】前記不正検出ステップでは、該読履歴の各レコードが所定の管理センタC Aの公開鍵P<sub>CA</sub>で暗号化されている場合には、該読履歴に含まれる各レコードを最新のものから順に該管理センタC Aの秘密鍵S<sub>CA</sub>によって復号化して検査し、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを特徴とする請求項20に記載の情報処理方法。

【請求項26】他の装置にコンテンツを譲渡する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータソフトウェアは、コンテンツ譲渡側の装置と相互認証するステップと、コンテンツ譲渡側の装置固有情報S I D、コンテンツ譲渡側の装置固有情報R I D、コンテンツ受信側が発生したノンスT N、並びにコンテンツの譲渡履歴全体に対する電子署名T S Gを含んだ新規レコードを追加してコンテンツの譲渡履歴を更新するステップと、コンテンツの譲渡履歴をコンテンツ譲渡側の装置に送信するステップと、前記相互認証並びにコンテンツ譲渡側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲渡側の装置に送信するステップと、を具備することを特徴とする記憶媒体。

【請求項27】他の装置からコンテンツを譲受する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータソフトウェアは、コンテンツ譲渡側の装置と相互認証するステップと、コンテンツ譲渡側の装置にノンスT Nを送信するステップと、コンテンツ譲渡側の装置固有情報S I D、コンテンツ譲受側の装置固有情報R I D、コンテンツ譲受側が発生したノンスT N、並びに、コンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名T S Gを含むレコードからなるコンテンツの譲渡履歴をコンテンツの譲渡側の装置から受信するステップと、該読履歴の最後のレコードにコンテンツ譲渡側の装置固有情報S I D、コンテンツ譲受側の装置固有情報R I D、自身が生成したノンスT Nが含まれていること、及び/又は、電子署名T S Gが正しく該読履歴に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査するステップと、を具備することを特徴とする記憶媒体。

【請求項28】前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタC Aの公開鍵P<sub>CA</sub>を用いて暗号化したもので置換する、ことを請求項27に記載の特徴とする記憶媒体。

【請求項29】複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記譲渡履歴は、コンテンツ固有の情報T I Dと、コンテンツを譲渡する度に追加されるレコードと、を含み、

前記コンピュータソフトウェアは、コンテンツ及び譲渡履歴を受信するステップと、同じコンテンツ固有情報T I Dを持つコンテンツを2回以上受信したことに応じて、譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする記憶媒体。

【請求項30】前記不正検出ステップでは、該読履歴の各レコードが所定の管理センタC Aの公開鍵P<sub>CA</sub>で暗号化されている場合には、該読履歴に含まれる各レコードを最新のものから順に該管理センタC Aの秘密鍵S<sub>CA</sub>によって復号化して検査し、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを請求項29に記載の特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、乗車券、入場券、会員所、許可書、サービス券などの電子チケットを始めとする各種のデジタル情報を不正利用から保護する情報処理装置及び方法、並びに記憶媒体に係り、特に、デジタル情報を耐久性のあるハードウェア上に保持することによって複数の機器間でデジタル情報の譲渡を繰り返す過程において不正利用から保護する情報処理装置及び方法、並びに記憶媒体に関する。

【0002】更に詳しくは、本発明は、デジタル情報を複数の機器間で譲渡を繰り返す過程において万一ある機器ハードウェアが解析・改変された場合であってもデジタル情報不正利用から保護する情報処理装置及び方法、並びに記憶媒体に係り、特に、ハードウェアの解析・改変によるデジタル情報の不正利用を検出することによってハードウェアの解析・改変への潜在的な意図を抑制する情報処理装置及び方法、並びに記憶媒体に関する。

【0003】

【従来の技術】昨今の情報処理、情報通信技術の急速な

進歩に伴い、あらゆる情報がデジタル化されてコンピュータ上で取り扱うことができるようになり、さらには、コンピュータ・ネットワークやメディアを媒介として複数のシステム間で情報が共有・流通されるようになってきている。また、インターネットの爆発的な普及に伴い、デジタル情報を即時的に配信・配布することが可能となっている。すなわち、遠い距離離れた場所に存在する情報資源であっても、それがデジタル化するなわちコンピュータライズされてさえいれば、何処からでも容易且つ瞬時に取得することができる。例えば、映像や音楽などのコンテンツや、コンサートのチケットなどはデジタル化され、ネットワーク上で流通・販売されている。いまやデジタル情報は、それ自身が経済価値のある取引の対象なのである。

【0004】しかしながら、情報の伝達と共有の容易性というデジタル情報本来の利点も、その応用範囲の拡大によって、新たな問題が発生してきている。何故ならば、デジタル形式の情報の複製や改竄は極めて容易であり、さまざまな不正行為による危害に無防備にさらされるからである。とりわけ、ソフトウェアや音楽情報などの著作権によって保護されるべき情報や、証明書や有価証券など唯一性が重要な情報に関しては、著作権法やその他の情報の複製・改竄に関する法規制を強化するだけでは不十分であり、情報技術の観点からも保護を拡充する必要があると思われる。

【0005】従来であれば、例えば音楽情報はCDやレコードなどのメディアに記録して流通・販売されていた。これら記録メディアからの完全な複製は技術的に困難であるため、複製利用が大きな問題とはならなかった。しかしながら、近年、情報を複製するツールでもあるパーソナル・コンピュータ（PC）や周辺機器が発達し一般消費者でも安価に入手できるようになってきたため、それら記録メディアから完全な形態でデジタル情報を抽出することができ、扱い易く加工することを容易にすることができた。また、このようにして得られた音楽情報が、ネットワークを通じて不特定多数に不正に配信されてしまうという状況が生じている。このことは、音楽などコンテンツの制作者又はその著作権者や、これら情報コンテンツを商品としてきた産業界に大きな脅威を与える。情報コンテンツの不正利用の横行を許容すれば、音楽等のコンテンツ制作者やソフトウェア開発者は新たな創作意欲を喪失し、産業活動自体が沈滞してしまかねない。

【0006】一方、乗車券、入場券、会員券、許可書、サービス券などの証明書や有価証券は、いままでは、容易に複製・偽造されないように特殊な加工（例えば、透かしや特殊印刷や機械・捺印など）が施された紙やその他の媒体を用いて、その上に証明書や有価証券としての情報を記録していた。証明書や有価証券としての情報自体が複製されても、それを記録した媒体である紙が存在

しなければ（すなわち特殊加工が施されなければ）、情報の効力を持たなくすることによって、証明書や有価証券が表す価値の複製を防いだ。

【0007】この種の証明書や有価証券に関しても、デジタル情報化することにより、いわゆる「電子チケット」という形態で、コンピュータ・ネットワーク上で流通・販売することができる。例えば、コンサートのチケットや航空券などは、電話網やコンピュータ・ネットワークを結んで予約することは従来も可能であるが、最終的なチケットの受け取りは郵送や手渡しに委ねられていた。これに対し、電子チケットによれば、予約と購入を同じ手続で済ませることができるので、消費者は店舗に向かう手間が省け、販売者にとってはチケットの流通コストや管理コストなどを削減することができ利益の増大につながる。すなわち、電子チケットによれば、デジタル情報化による伝達の利便性を活かすことができる。しかしながら、電子チケットを普及させるためには、音楽などのデジタル・コンテンツの場合と同様に、デジタル情報の複製や改竄を技術的に確保する必要がある。

【0008】このため、最近では複製を防ぎながら電子情報を扱うことができるシステムに関して数多くの提案がなされている。

【0009】デジタル情報の保護には、所定の暗号鍵を用いて暗号化したコンテンツを流通・販売するというシステムが一般的であり、既に広汎に採用されている。例えば、暗号鍵の販売という形式で情報の利用に対して課金を行うことができる。但し、暗号鍵の流通・配布のため、暗号鍵自体もデジタル化してしまうことが多い。このような場合、コンテンツやチケットなど本来の流通・販売の対象である情報と同様に、暗号鍵も複製や改竄が容易になってしまうので、これを技術的に保護しなければならない。

【0010】例えば、本出願人に既に譲渡されている特開平11-328850号公報には、コンテンツの保護を充分図るとともに正当な課金を行うことができる情報配信システムについて開示されている。同公報によれば、コンテンツ・サーバには、Cキーにより暗号化されたコンテンツとCキーとが蓄積されるコンテンツ・データベースが設けられていて、このCキーにより暗号化されたコンテンツとCキーをMキーで暗号化して、ユーザ・マシンに送る。ユーザ・マシン上では、Cキーにより暗号化されたコンテンツとCキーをストレージ・デバイスに保存する。そして、再生時にストレージ・デバイスからのCキーにより暗号化されたコンテンツとCキーを暗号化/復号化処理チップに送出して復号するとともに、Cキーに応じて課金を行う。また、Cキーには、時間の経過とともに動的に変化するD Aコードを付加しておく。このようなD Aコードを付加することで、Cキーを盗置させておいて、コンテンツを不正利用することが防止できるとともに、D Aコードを利用して、コ

コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借することができる。

【0011】同公報では、比較的大きな電子情報を扱う方法が示されているため、電子情報は複製や改竄されないように暗号化されてハード・ディスクなどの一般の記憶装置に保持される。但し、暗号化の鍵は保持装置のハードウェアに組み込まれているので、読み出すことができない。したがって、保持されている電子情報を読み出しても、電子情報を復号化して用いることはできない。電子情報を使うときには、ハードウェアの回路内でだけ復号化して利用され、外部には復号化された電子情報は漏れないようになっている。ハードウェアで保護したい電子情報の利用を制限し、それによって複製されることを防いでいる。

【0012】また、ICカードを用いたようなセキュリティシステムの場合には、ICカード間で鍵を配布・交換することによって、情報のセキュリティをハードウェア的に維持するようになっている。ICカードに内蔵された電子情報が勝手に読み書きできない(又は耐タンパ性を備えた)半導体メモリ上に鍵などの情報が保持され、認証鍵を知るものだけが読み書きできる。そのため認証鍵を利用するものが、ICカード上の電子情報を複製することなく移動することを注意深く行うことにより、電子情報をICカード間でやり取りしつつ、その複製を防ぐことができる。例えば、別のICカードに情報を移動させたときには、必ず元のICカードの内容を削除するようにする(通常ハードウェアで実現する)。

【0013】また、ソニー株式会社が提供するシステム「MagicGate Memory Stick」では、ICカードに類似した仕組みによる情報セキュリティを実用化している。このMagicGateでは、まずICカード相互間で認証した後、一方の装置から他方の装置に鍵を明渡し、最後に元の装置から鍵を消去するようになっている。こうしたシステムでは、デジタル情報としての移動の容易性を依然として維持しつつ、複製や改竄の容易さという性質の制限を実現することができる。

【0014】ICカードなどの特定のハードウェアを用いてデジタル情報を保護するシステムにおいては、ハードウェアの解析・改竄に対する耐久性(耐タンパ性)が確保されていることが重要な前提となる。上述したように、デジタル情報を複製、改竄されないように保持する仕組みは大きな利点があり、今後とも活用されていく技術であると考えられるので、ハードウェアの耐久性が破られぬように解析・改竄がより困難なハードウェアを開発し採用する必要がある。

【0015】しかしながら、ハードウェアは人工物であり、完全とは言い難い。すなわち、コストを払えば(あるいは、鍵を破るにより得られるデジタル情報にコストを回収するだけの経済的価値が見出されるならば)、鍵を破ることは不可能ではない。このため、

単にハードウェアの耐久性を向上させるだけではなく、万一解析・改竄された場合にはそれが検出できること、さらにはその結果の不正による被害を食い止められることが重要となる。

【0016】特に、ハードウェアの耐久性を充分に高めた場合、それに対する解析・改竄は計画的、組織的なものとならざるを得ない。の場合にも、解析・改竄を行うか否かは、その結果として可能になる情報の不正利用によってコストを回収できるか(すなわち情報の経済的価値)が重要になる。したがって、解析・改竄によって可能となる不正が容易に検出され不正者を特定できるということは、言い換えればこうした情報の不正利用のやり取りを困難なものにし、結果としてハードウェアの解析・改竄への潜在的な意図を抑制するのに非常に効果的であると思考される。

【0017】

【発明が解決しようとする課題】本発明は、上述したような技術的課題を鑑みたものであり、ハードウェアの不正解析がなされ、その結果として複製されないように保持されていたデジタル情報の複製が可能になり、それが比較的大規模に流通した場合に、そのことが検出でき、さらにどのハードウェアが不正解析されたかが特定できる仕組みを提案することを目的とする。

【0018】その仕組みは、最初に個々のコンテンツに唯一性を持たせて流通させ、後にコンテンツを回収した際に、複数の同一コンテンツが発見された場合には、流通の過程でコンテンツの複製が行われたことが判ることである。さらに、それぞれのコンテンツに談話履歴を付随させて、複数の保持装置への談話がどの時点で発生したかを調べることで可能である。

【0019】

【課題を解決するための手段及び作用】本発明は、上記課題を参照してなされたものであり、その第1の側面は、装置間でコンテンツを交換する情報処理装置であって、コンテンツ及びコンテンツの談話履歴を送信及び/又は受信する通信手段と、装置固有の情報を保管する固有情報保持手段と、コンテンツを交換する相手側の装置と相互認証する認証手段と、コンテンツを保持するコンテンツ保持手段と、コンテンツの談話履歴を管理する談話履歴管理手段と、を具備することを特徴とする情報処理装置である。

【0020】ここで、前記認証手段は、例えば、コンテンツを交換する相手側の装置との間で互いの電子署名を用いた認証を行うことができる。

【0021】また、前記談話履歴管理手段は、コンテンツ受信時にはノンストNを発生し、コンテンツ送信時には、コンテンツ送信側の装置固有情報R ID、コンテンツ受信側の装置固有情報R ID、コンテンツ受信側が発生したノンストN、並びにコンテンツの談話履歴全体に対する電子署名TSGを含んだ新規レコードをコンテン



ツの読取履歴に追加するようにして、コンテンツの移動に関する記録である読取履歴をとるようにする。

【0022】したがって、前記読取履歴管理手段は、コンテンツ受信時に、コンテンツに付随する読取履歴の最後のレコードにコンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、自身が生成したノンスTNが含まれていること、及び／又は、電子署名TSGが正しく読取履歴全体に対するコンテンツ送信側の装置の署名になっていることを確認することによって、コンテンツの読取履歴を検査することができる。

【0023】また、読取履歴を、コンテンツの読取履歴全体に対する電子署名TSGをレコードに含めるという一種の「入れ子構造」とすることにより、それぞれのコンテンツ交換時に必要な読取履歴検査のために必要な計算のうち、計算処理量の大きい公開鍵暗号の処理回数が読取回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による読取履歴の改竄に対する耐久性をも実現することができる。

【0024】また、前記読取履歴管理手段は、コンテンツ送信側から受信側へ以前のコンテンツ読取に対応する暗号化されている読取履歴に未だ暗号化されていない新規レコードを追加したものを送るようにしてもよい。このような場合、コンテンツ受信側の装置では、未だ暗号化されていない新規レコードを検査した後に、所定の管理センタCA (Certification Authority) の公開鍵P<sub>CA</sub>を用いて暗号化して、コンテンツの読取履歴の未だ暗号化されていない新規レコードを暗号化したものに置き換えるようにしてもよい。このような場合、読取履歴を所定のシステム管理者CA以外には読めないようにすることができるので、システム管理者には不正が行われた情報処理装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどの情報処理装置を経由してきたかを秘密にすることができる。

【0025】前記認証手段によって相手側の装置と相互認証でき、さらに、前記読取履歴管理手段によりコンテンツの読取履歴の正当性が確認できた場合にのみ、コンテンツの交換を行うようにすることで、正当なコンテンツの流通とコンテンツの保護を確保することができる。この結果、音楽や映像情報などのように経済価値を持つコンテンツや、証明書や有価証券などのように唯一性が重要なコンテンツ (電子チケット) などのデジタル情報を複数の装置にまたがって安全に移動させることができる。

【0026】また、本発明の第2の側面は、複数の装置間読取履歴を伴って流通されたコンテンツを回収する情報処理装置であって、前記読取履歴は、コンテンツ固有の情報TIDと、コンテンツを読取る度に追加されるレコードと、を含み、前記情報処理装置は、コンテン

ツ及び読取履歴を受信する通信手段と、読取履歴を検査してコンテンツの流通過程における不正を検出する不正検出手段と、を具備することを特徴とする情報処理装置である。

【0027】読取履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置が発生したノンスTN、並びに、そのレコードより以前に追加されたすべてのレコードを含むコンテンツの読取履歴全体に対するコンテンツ送信側の装置による電子署名TSGを含んでいる。

【0028】したがって、前記不正検出手段は、読取履歴に含まれる各レコードの電子署名を最新のレコードから遡りながら検証する。そして、整合しない電子署名のあるレコードを発見した場合には、そのレコードのコンテンツ受信側の装置、すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0029】また、読取履歴が所定の所定の管理センタCAの公開鍵P<sub>CA</sub>で暗号化されている場合には、前記不正検出手段は、読取履歴に含まれる各レコードを最新のものから順に該管理センタCAの秘密鍵S<sub>CA</sub>によって復号化して検査するようにする。そして、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合には、該レコードを受信した装置すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0030】また、読取履歴の先頭レコードに含まれるSIDがコンテンツを発行する所定の装置を示していない場合には、該SIDによって識別される装置を不正者として特定することができる。

【0031】また、前記不正検出手段は、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信した場合には、各コンテンツが持つ読取履歴を比較して、枝分かれレコードを探索する。ここで言う「枝分かれレコード」とは、同じコンテンツ固有情報TIDを持つコンテンツに付随する読取履歴が、正しくコンテンツ発行装置を示す装置固有情報SIDのレコードから始まり、途中のレコードまで同一のレコードを持ち、あるレコードから異なる始める場合に、最初の異なるレコードのことを示す。そして、発見された枝分かれレコード中のコンテンツ送信側の装置固有情報SIDによって識別される装置を不正者として特定することができる。

【0032】また、本発明の第3の側面は、他の装置にコンテンツを読取る情報処理方法であって、コンテンツ読受側の装置と相互認証するステップと、コンテンツの読取履歴を更新するステップと、コンテンツの読取履歴をコンテンツ読受側の装置に送信するステップと、前記相互認証並びにコンテンツ読受側の装置からの読取履歴の確認後にコンテンツをコンテンツ読受側の装置に送

信するステップと、を具備することを特徴とする情報処理方法である。

【0033】前記のコンテンツの読取履歴を更新するステップでは、コンテンツ読取側の装置固有情報SID、コンテンツ読取側の装置固有情報RID、コンテンツ受信側が発生したノンスTN、並びにコンテンツの読取履歴全体に対する電子署名TSGを含んだ新規レコードをコンテンツの読取履歴に追加する。

【0034】したがって、コンテンツ読取時において、コンテンツに付随する読取履歴の最後のレコードにコンテンツ読取側の装置固有情報SID、コンテンツ読取側の装置固有情報RID、自身が生成したノンスTNが含まれていること、及び/又は、電子署名TSGが正しく読取履歴全体に対するコンテンツ読取側の装置の署名になっていることを確認することによって、コンテンツの読取履歴を検査することができる。

【0035】また、読取履歴をコンテンツの読取履歴全体に対する電子署名TSGをレコードに含めるといった一種の入れ子構造とすることにより、それぞれのコンテンツ交換時に必要な読取履歴検査のために必要な計算のうち、計算処理量の大きい公開鍵符号の処理回数が読取回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による読取履歴の改竄に対する耐久性を実現することができる。

【0036】前記のコンテンツの読取履歴を更新するステップでは、コンテンツ送信側から受信側に、これまでのコンテンツ読取側に対応する暗号化された読取履歴に未だ暗号化されていない新規レコードを追加したものを送る。これに対し、コンテンツ受信側では、新規レコードを検査した後、それを所定の管理センタCAの公開鍵P<sub>CA</sub>を用いて暗号化した後に、コンテンツの読取履歴の未だ暗号化されていない新規レコードを暗号化したもので置換するようにしてもよい。このような場合、読取履歴を所定のシステム管理者以外には読めないようにすることができ、システム管理者には不正が行われた情報処理装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどの情報処理装置を経由してきたかを秘密にすることができる。

【0037】また、本発明の第4の側面は、他の装置からコンテンツを読受する情報処理方法であって、コンテンツ読取側の装置と相互認証するステップと、コンテンツ読取側の装置にノンスTNを送信するステップと、コンテンツの読取側の装置からコンテンツの読取履歴を受信するステップと、受信した読取履歴を検査するステップと、コンテンツ読取側の装置からコンテンツを受信するステップと、を具備することを特徴とする情報処理方法である。

【0038】読取履歴の各レコードは、コンテンツ読取側の装置固有情報SID、コンテンツ読取側の装置固有

情報RID、コンテンツ読取側の装置が発生したノンスTN、並びに、そのレコードよりも以前に追加されたすべてのレコードを含むコンテンツの読取履歴全体に対するコンテンツ読取側の装置による電子署名TSGを含んでいる。

【0039】したがって、前記の読取履歴を検査するステップでは、読取履歴の最後のレコードにコンテンツ読取側の装置固有情報SID、コンテンツ読取側の装置固有情報RID、自身が生成したノンスTNが含まれていること、及び/又は、電子署名TSGが正しく読取履歴全体に対するコンテンツ読取側の装置の署名になっていることを確認することによって、コンテンツの読取履歴を検査し、コンテンツの流通過程における不正行為のあったコンテンツの受け取りを拒否する。

【0040】また、読取履歴はコンテンツの読取履歴全体に対する電子署名TSGをレコードに含めるという一種の入れ子構造となっているので、それぞれのコンテンツ交換時に必要な読取履歴検査のために必要と計算のうち、計算処理量の大きい公開鍵符号の処理回数が読取回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による読取履歴の改竄に対する耐久性を実現することができる。

【0041】コンテンツの読取履歴が暗号化されている場合、コンテンツの読取側から、それ以前の読取側に対応するすべてのレコードを暗号化したものからなる読取履歴に、今回の読取側に対応する未だ暗号化されていない新規レコードが追加されたものを受け取る。コンテンツ読取側では、この新規レコードを検査して、該レコードが正しい場合には、それを所定の管理センタCAの公開鍵P<sub>CA</sub>で暗号化する。そして、読取履歴の暗号化されていない新規レコードをこの暗号化したもので置換する。これにより、CAなどのシステム管理者以外がコンテンツの流通経路の秘密を知り得るということを防止することができる。

【0042】また、本発明の第5の側面は、複数の装置間で読取履歴を伴って流通されたコンテンツを回収する情報処理方法であって、前記読取履歴は、コンテンツ固有の情報RIDと、コンテンツを読取する度に追加されるレコードと、を含み、コンテンツ及び読取履歴を受信するステップと、読取履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする情報処理方法である。

【0043】読取履歴の各レコードは、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側の装置が発生したノンスTN、並びに、そのレコードよりも以前に追加されたすべてのレコードからなるコンテンツの読取履歴に対するコンテンツ送信側の装置による電子署名TSGを含んでいる。

【0044】したがって、前記不正検出ステップでは、該読履歴に含まれる各レコードの電子署名を最新のレコードから遡りながら検証して、整合しない電子署名をしたコンテンツ送信側の装置を不正者として特定することができる。

【0045】また、該読履歴が所定の所定の管理センタCAの公開鍵 $P_{CA}$ で暗号化されている場合には、前記不正検出ステップでは、該読履歴に含まれる各レコードを最新のものから順に該管理センタCAの秘密鍵 $S_{CA}$ によって復号化して検査するようにする。そして、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合には、該レコードを受信した装置すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0046】また、前記不正検出ステップでは、該読履歴の先頭レコードに含まれるSIDがコンテンツを発行する所定の装置を示していない場合には、該SIDによって識別される装置を不正者として特定することができる。

【0047】また、前記不正検出ステップでは、同じコンテンツ固有情報TIDを持つコンテンツを2回以上受信した場合には、各コンテンツが持つ該読履歴を比較して、枝分かれするレコードを探索する。ここで言う「枝分かれレコード」とは、同じコンテンツ固有情報TIDを持つコンテンツに付随する該読履歴が、正しくコンテンツ発行装置を示す装置固有情報SIDのレコードから始まり、途中のレコードまで同一のレコードを持ち、あるレコードから異なる場合に、最初の異なるレコードのことを示す。そして、発見された枝分かれレコード中のコンテンツ送信側の装置固有情報SIDによって識別される装置を不正者として特定することができる。

【0048】しかし、本発明に係る情報処理装置又は方法によれば、最初に個々のコンテンツに唯一性を持たせて流通させ、後にコンテンツを回収した際に、複数の同一コンテンツが発見された場合には、流通の過程でコンテンツの複製が行われたことが判る。さらに、それぞれのコンテンツに該読履歴を付随させて、複数の保持装置への該読履歴がどの時点で発生したかを調べることができる。

【0049】これに類似する技術は、該読可能な電子現金の方法の一部として既に提案されている。例えば、T. Okamoto et al 著の "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash" (Advances in Cryptology Crypto'89, Lecture Notes in Computer Science 435, pp. 481-496, Springer-Verlag, Berlin (1989)) や、日本国特許第2027713号「電子現金実施方法及びその装置」、D. Chaum及びT. P. Pedersen著の "Transferred Cash Gross in Size" (Advances in Cryptology Eurocrypt'92, Lecture Notes in Computer Science, pp.

390-407, Springer-Verlag, Berlin (1992)) などでは、電子現金に関する手法が記述されている。これらの電子現金の場合には、デジタル情報として表される現金が多重に支払われることを阻止する方法が採用されている。しかし、これらの文献に記載された方法では、コンテンツすなわち電子現金の該読の際に、付随する該読履歴のすべての検査を行う必要がある。つまり、該読の回数に比例した計算量が必要であり、該読回数が増えた場合に、計算量が膨大になるという欠点がある。また、これら上述の文献はいずれも、電子現金という使用目的に特化した方法であり、音楽コンテンツなどの一般のコンテンツ流通に適用することは難しい。

【0050】これに対し、本発明に係る情報処理装置及び方法では、該読履歴のデータ構造を入れ子構造とすることで、各該読時に必要な該読履歴検査のための計算量を該読回数に依存しない定値としながら、該読途中での不正者による該読履歴の改竄に対する耐久性をも実現することができる。

【0051】例えば、個々のコンテンツ毎に区別が付き、不正がない限りシステム内にそれぞれが唯一存在し、一定期間の後に回収されるような条件を満たすコンテンツに対しては、本発明を容易に適用することができる。

【0052】また、本発明の第6の側面は、他の装置にコンテンツを該読する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータソフトウェアは、コンテンツ該読側の装置と相互認証するステップと、コンテンツ該読側の装置固有情報SID、コンテンツ該読側の装置固有情報RID、コンテンツ受信側が発生したノンスTN、並びにコンテンツの該読履歴全体に対する電子署名TSGを含む新規レコードを追加してコンテンツの該読履歴を更新するステップと、コンテンツの該読履歴をコンテンツ該読側の装置に送信するステップと、前記相互認証並びにコンテンツ該読側の装置からの該読履歴の確認後にコンテンツをコンテンツ該読側の装置に送信するステップと、を具備することを特徴とする記憶媒体である。

【0053】また、本発明の第7の側面は、他の装置からコンテンツを該読する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータソフトウェアは、コンテンツ該読側の装置と相互認証するステップと、コンテンツ該読側の装置にノンスTNを送信するステップと、コンテンツ該読側の装置固有情報SID、コンテンツ該読側の装置固有情報RID、コンテンツ該読側の装置が発生したノンスTN、並びに、コンテンツの該読履歴全体に対するコンテンツ該読側の装置による電子署名TSGを含むレコードからなるコンテンツの該読履歴をコンテンツの

誹謗側の装置から受信するステップと、誹謗履歴の最後のレコードにコンテンツ誹謗履歴の装置固有情報TS IDコンテンツ誹謗受信の装置固有情報RID、および生成されたノンスTNが書き込まれていること、及び/又は、電子署名名TS Gが正しく誹謗履歴に存在するコンテンツ誹謗側の装置の署名になっていることを確認することによって、コンテンツの誹謗履歴を検査するステップと、コンテンツ誹謗側の装置からコンテンツを受信するステップと、を具備することを特徴とする情報媒体である。

【0054】前記の議決履歴を検査するステップでは、コンテンツの議決履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタCAの公開鍵P<sub>CA</sub>を用いて暗号化したもので置換するようにしてもよい。

【0055】また、本発明の第8の側面は、複数の装置間で読取履歴を伴って流通させたコンテンツを回収する処理をコンピュータ上で実行するように記述されたコンピュータソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記読取履歴は、コンテンツ固有の情報TIDと、コンテンツを読取る度に追加されるワードと、を各々、前記コンピュータソフトウェアは、コンテンツ及び読取履歴を受信するステップと、同じコンテンツ及び情報TIDを持つコンテンツを2回以上受信したことに応じて、読取履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする記憶媒体である。

【0056】前記不正検出ステップでは、読取履歴の各レコードが所定の管理センタCの公開鍵P<sub>Ca</sub>で暗号化されている場合には、読取履歴に含まれる各鍵コードを最新のものから順に該管理センタCの秘密鍵S<sub>Ca</sub>によって復号化して検査して、正しく復号化できない、あるいは署名を正しく検証できないコードを検出した場合に、該レコードを受信した装置を不正者として特定するようにしてもよい。

【10057】本発明の第6乃至第8の各側面に係る記憶媒体は、例えば、様々なプログラムコードを実行可能な汎用コンピュータシステムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、CD (Compact Disc) やFD (Floppy Disk)、MO (Magnet-Optical disc) などの半導体自在で可逆性の記憶媒体である。あるいは、ネットワーク (ネットワークは無線、有線の区別を問わない) などの伝送媒体などを經由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供するなどの技術的に可能である。

【0058】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働関係を定義したもので

ある。換言すれば、本発明の第6乃至第8の各側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアを所定のコンピュータ上にインストールすることによって、該コンピュータ上では協働的作用が発揮され、本発明の第3乃至第5の各側面に係る情報処理方法と同様の作用効果を得ることができる。

【0059】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0060】

【発明の実施の形態】本発明の実施形態について記述する前に、まず、本発明において用いられる暗号技術上の幾つかの用語について説明する。

【0061】共通鍵暗号

本発明では、「共通鍵暗号」と呼ばれるアルゴリズムと、「公開鍵暗号」、「電子署名」と呼ばれるアルゴリズムを利用する。共通鍵暗号は「対称暗号」とも呼ばれ、データを暗号化する際に用いる鍵と復号化する際に用いる鍵が同じ、あるいは異なる場合でも一方から他方を算出することが容易であるという性質を持った暗号アルゴリズムである。代表的な共通鍵暗号アルゴリズムとしては、アメリカ合衆国商務省情報局が標準暗号として認定した「DES (data encryption standard)」や「Triple DES」、NTTの「FEAL (fast data encryption algorithm)」などを挙げることができる。以下では、共通鍵Kによりmを暗号化して、暗号文cを得る場合を $c = E(k, m)$ と表現し、また、その復号化を $m = D(k, c)$ と表現することとする。この場合、KとK'が一致すれば、mとm'も一致することとする。

【0062】公園鍵暗号

公開鍵暗号は「非対称暗号」とも呼ばれ、データを暗号化する際に用いる鍵と復号する際に用いる鍵が異なり、且つ、一方から他方を算出することが非現実的困難であるという性質を持った暗号アルゴリズムである。この公開鍵暗号アルゴリズムによれば、一方の鍵で暗号化した情報は、他方の鍵でしか復号できないことができる。暗号化の鍵は「公開鍵」と呼ばれ、一般に公開して誰でも使用できることになる。また、復号化の鍵は「秘密鍵」と呼ばれ、他人に漏れないように所有者が管理する。これによって、任意の送手は公開鍵で暗号化することによって、秘密鍵を所持する受け手しか復号化することができない暗号文を送信することができる。公開鍵を  $P_k$ 、秘密鍵を  $S_k$  としたとき、公開鍵  $P_k$  によりデータ  $M$  を暗号化するときを  $C = E(P_k, M)$  と表現し、また、秘密鍵  $S_k$  により暗号文  $C$  を復号化するときを  $M = D(S_k, C)$  と表現する。重要な性質は、秘密鍵  $S_k$  を秘密に保てば、公開鍵  $P_k$  や暗号文  $C$  が知られたとしても、元の平文  $M$  が得られないという点である。公開鍵暗号アルゴリズムとしては、「RSA (Rivest, Shamir, Adleman)

ir Adleman)「暗号や、楕円曲線暗号などが知られている。

### 【0063】電子署名

電子署名は、データ通信における印鑑やサインに相当する機能であり、受け取った情報が確かに送り手が送ったものであることを保証したり(偽造防止)、受け手が受け取った情報の内容が勝手に書き替えたり、その内容が送られてきた内容だと言い張れないようにする(改竄防止)、などの目的で使用される。例えば、上述した公開鍵暗号アルゴリズムを応用することによって、電子署名を実現することができる。ここでは、RSA署名の場合を念頭に上で用いた公開鍵暗号の記法を用いて説明する。データMが存在するとき、Mの作成者が自分の秘密鍵 $S_k$ を用いて、電子署名 $SG(M) = D(S_k, h(M))$ を計算する。ここで、 $h(\quad)$ は一方方向性関数であり、出力値から入力値を知る(又は類推する)ことが非常に困難だという性質を持つ。こうした関数としては「MD5 (message digest algorithm 5)」や「SHA-1 (secure hash algorithm 1)」と呼ばれるものが挙げられる。データMを送る際に(M,  $SG(M)$ )の組で送ると、受け取り側は、 $h(M) = E(P_k, SG(M))$ が満たされるかどうかを確認することで、Mが改竄されていないことと、電子署名 $SG(M)$ が秘密鍵 $S_k$ の所有者によって付加されたものであることを確認することができる。すなわち、メッセージ作成者が自分の秘密鍵でメッセージを暗号化することにより、暗号化メッセージの受け取り手は作成者の公開鍵でしか復号化できないので、メッセージすなわち署名の偽造や改竄ができない。以下、このような手続きのことを「署名確認」と呼ぶ。電子署名としては、RSA署名やElGamal署名、楕円EIGamal署名などが挙げられる。電子暗号との混同を避けるために、署名生成に使う秘密鍵 $S_k$ のことを「署名生成鍵」と呼び、署名検証に使う公開鍵 $P_k$ のことを「署名検証鍵」と呼ぶ。また、署名生成鍵、署名検証鍵と記述する場合には、署名で使用する一方方向性関数を特定する情報も含まれているものとする。

【0064】チャレンジ&レスポンス認証  
チャレンジ・コードと呼ばれる1回限りの数字(タイムスタンプや乱数など)を基に認証を安全に実施する手法である。公開鍵暗号アルゴリズムを応用することにより、チャレンジ&レスポンス認証を実現することができる。公開鍵 $P_k$ を使って、相手が秘密鍵 $S_k$ を所有することを、秘密鍵自体を知ることなく確認することができる。例えば、検証側で乱数 $r$ を生成し、 $r' = E(P_k, r)$ を計算して相手に送る。これに対し、相手が正しく元の乱数 $r = D(S_k, r')$ を計算して検証側に返すことによって、検証側では相手が $S_k$ を所有していることを確認できる。あるいは、検証側から乱数 $r$ を相手に送り、相手が $r' = D(S_k, h(r))$ を計算して返す。

これに対し、検証側では、 $h(r) = E(P_k, r')$ が成り立てば、相手が秘密鍵 $S_k$ を所有していることが確認される。同様に電子署名の手法により、署名検証鍵 $P_k$ を使って、相手が署名生成鍵 $S_k$ を所有することを、署名生成鍵自体を知ることなく確認することができる。すなわち、検証側から乱数 $r$ を生成し相手に送る。これに対し、相手が $SG(r) = D(S_k, h(r))$ を計算して返す。そして、検証側では、 $h(r) = E(P_k, SG(r))$ が成立すれば、相手が署名生成鍵 $S_k$ を所有していることが確かめられる。チャレンジ&レスポンス認証により、特定の秘密鍵あるいは署名生成鍵が存在することを、対応する公開鍵あるいは署名検証鍵を用いて、秘密鍵あるいは署名生成鍵自体を知ることなく確認することが可能である。

### 【0065】証明書

特定の相手を認証する(あるいは、特定の相手だけに情報を伝える、特定の相手が作成した文書であることを確認する)ためには、相手が所有する秘密鍵に対応する公開鍵、あるいは署名生成鍵に対応する署名検証鍵を正しく把握していることが重要である。しかし、そうした相手が多い場合には、すべてを把握しておくことは困難である。このために、1つだけ正しい署名検証鍵を把握していれば、それを基にして、他の公開鍵あるいは署名検証鍵を連鎖的に正しく把握する方法が提案されている(ITU-TのX.509勧告)。1つだけ把握すべき署名検証鍵に対応する署名生成鍵の所有者のことを、一般に「認証センター(CA: Certification Authority)」と呼ぶ。CAは、公開鍵が間違いないく所有者本人のものであることを証明可能な第3者機関であり、公正かつ中立な立場にあり、絶対的に信頼されるものであることを前提とする。CAは、CA自身の秘密鍵で暗号化した証明書を発行する。すなわち、証明書はCAの電子署名が付加されているので、他人が勝手に偽造することができない。CAの署名検証鍵 生成鍵の組を( $P_{CA}, S_{CA}$ )とし、署名検証鍵 $P_{CA}$ が公開されたシステムの参加装置に正しく伝えられている署名検証鍵であるとする。また、署名生成鍵 $S_{CA}$ は、チケット・システム管理センターだけが使用できるとする。それ以外の公開鍵あるいは署名検証鍵 $P_k$ に関しては、その所有者と結びつく情報 $Inf_{o_n}$ と $P_k$ を組にしたもの( $Inf_{o_n}, P_k$ )は、CAが署名生成鍵 $S_{CA}$ を使って生成した署名 $S_n = D(S_{CA}, h(Inf_{o_n}, P_k))$ を付加した証明書( $Inf_{o_n}, P_k, S_n$ )を発行する。これによって、CAが $Inf_{o_n}$ で特定される所有者と $P_k$ の関係を保証したことになる。

### 【0066】証明書検証

証明書を利用する際には、秘密鍵又は署名生成鍵 $S_k$ の所有者は、最初に証明書( $Inf_{o_n}, P_k, S_n$ )を署名検証側に示す。検証側は、CAの公開鍵 $P_{CA}$ を用いて証明書の署名確認を行うことによって( $h(Inf_{o_n},$

$n, P_n) = E(P_{cn}, SG_n))$ 、証明書の正当性を検証する。この結果、 $Inf_{o_n}$ の示す内容が $P_n$ で認証できる(公開鍵 $P_n$ に対応する秘密鍵 $S_n$ を持つ、又は、署名検証鍵 $P_n$ に対応する署名生成鍵 $S_n$ を持つ)相手と結びつくことを確認することができる。例えば、 $Inf_{o_n}$ が人名であれば、 $P_n$ で認証できる相手の人名が判明する。証明書には、一般には、暗号のアルゴリズムや、使用されている一方方向関数の種類の情報も含まれる。以下の説明で証明書について区別が必要である場合、電子署名の検証鍵に関するものである場合は「署名証明書」と呼び、公開鍵暗号の公開鍵に関するものである場合には「鍵証明書」と呼ぶことにする。また、証明書の情報は $Inf_{o_n}$ で伝えられるべき内容がなない場合であっても、 $P_n$ で認証できる相手がCAに登録されていることを確認する目的で、証明書検証アルゴリズムが用いられる場合もある。

【0067】なお、本発明の要旨は、特定の暗号アルゴリズムに依存するものではない。以下の説明では、暗号アルゴリズムの一般的性質のみを用いて考案されている。したがって、説明中でも暗号の種類(共通鍵暗号、公開鍵暗号、電子署名)だけを記すことにする。

【0068】本発明は、ハードウェア機構を利用して、コンテンツを複製されないように流通させることのできるシステムに関するものである。本発明によれば、ICカードなどのシステム中のコンテンツ保持装置のハードウェアが不正に解析又は改変され、本来は唯一性が保たれるべきコンテンツが複製されたとき、同一コンテンツに関わる複数の流通経路から、コンテンツ保持装置に対する不正の有無を検出することができ、本発明によれば、さらに、コンテンツとともに流通する談履歴を用いることにより、どのコンテンツ保持装置で不正が行われたかを特定することができる。

【0069】本発明に関して、まず適用対象となるシステム、コンテンツ、装置、及びコンテンツ談履歴について説明する。次いで、コンテンツと一緒に流通する談履歴に関して、そのデータ構造、および談履歴を伴ったコンテンツ談履歴について説明する。次いで、不正検出のために必要と仮定を説明してから、コンテンツ保持装置に対する不正の有無の検出方法、さらに談履歴を用いて、どのコンテンツ保持装置で不正が行われたかを特定する方法について説明する。そして、本発明によって不正装置の特定が成功することを証明した後、最後に談履歴からコンテンツ流通の情報を収集されることで、コンテンツ流通の匿名性が失われることを防ぐために、談履歴を暗号化する方法について説明する。

【0070】1. 本発明適用のシステム

図1には、本発明の実施形態に係る、デジタル情報すなわちコンテンツを複製されないように保持するシステム1の構成を模式的に示している。このシステムは、コンテンツ保持装置10、コンテンツ発行装置30、コン

テンツ回収装置50の3種類からなる。コンテンツは、コンテンツ発行装置30で発行され、複数のコンテンツ保持装置10A、…、10N間でやり取りされ、最終的にコンテンツ回収装置50で回収される。

【0071】例えば、コンテンツ発行装置30は、チケットの発券装置に相当する。また、コンテンツ保持装置10は、ICカードなどチケットを購入した消費者が持ち運ぶ機器に相当する。同図において、複数のコンテンツ保持装置10A、…、10Nが直列的に並んでいるのは、コンテンツが各保持装置10A、…間で順次談渡されていくこと、すなわちコンテンツの流通を示している。あるコンテンツ保持装置が他のコンテンツ保持装置にコンテンツを成功裏に談渡したとき、元のコンテンツ保持装置からはコンテンツが消去される。また、コンテンツ回収装置50は改札などチケットを回収する装置に相当する。必ずしもすべてのコンテンツが回収される訳ではないが、イベントのチケットのように大部分が回収されると仮定する。コンテンツが電子チケットの場合、コンテンツには、その唯一性を示す固有番号が割り当てられ、さらには有効期限が設定されている。

【0072】本実施形態では、先述した同一システム1に属する各装置、すなわちコンテンツ保持装置10、コンテンツ発行装置30、並びにコンテンツ回収装置50の各々に対して、電子署名の証明書を発行するための管理センタ(CA)70が配置されている。その様子を図2に示している。

【0073】コンテンツ発行装置30、保持装置10、回収装置50は、それぞれに固有の公開鍵 $P_i$ と秘密鍵 $S_i$ を持つ。管理センタCA70に公開鍵 $P_i$ と装置の固有番号 $HID_i$ を登録することで、 $P_i$ と $HID_i$ が含まれる署名証明書( $Inf_{o_i}$ ,  $P_i$ ,  $SG_i$ )を発行してもらう。

【0074】ここで、署名証明書( $Inf_{o_i}$ ,  $P_i$ ,  $SG_i$ )中の $Inf_{o_i}$ には、対応する装置の固有番号 $HID_i$ が含まれるものとする。コンテンツの流通に関わる各装置10、30、50の所有者と $HID_i$ との対応は、管理センタCA70だけが把握しているものとする。コンテンツ発行者の署名証明書の場合には、 $Inf_{o_i}$ の一部として、コンテンツ発行者が否かを判断できる情報(例えば、チケットの場合であれば発行者名など)が含まれる。各装置10、30、50は、公開鍵 $P_i$ と秘密鍵 $S_i$ 、署名証明書( $Inf_{o_i}$ ,  $P_i$ ,  $SG_i$ )を保持する。

【0075】コンテンツ流通に関わる各装置10、30、50の所有者と $HID_i$ との対応は、管理センタCA70だけが把握していることで、特定の $HID_i$ で不正が行われたことが判った場合、管理センタCA70はその不正行為に関わった装置の所有者を追及することができる。また、各コンテンツに付随する談履歴(後述)によって、あるコンテンツが過去に $HID_i$ に対応する

保持装置10で保持されていたことが判った場合にも、具体的に誰がコンテンツを保持していたかを通常の利用者が知ることはできない。これにより、コンテンツ流通の匿名性が守られる。この点に関しては、後でさらに言及する。

【0076】以下では、説明の便宜上、コンテンツ発行装置30にはHID<sub>ISSUER</sub>が、コンテンツ回収装置50にはHID<sub>DEPOT</sub>がそれぞれ割り振られているものとする。また、コンテンツ発行者、コンテンツ回収者、コンテンツ保持者それぞれの署名名は、コンテンツ保持装置10、発行装置30、回収装置50において生成される署名のことを指す。コンテンツ回収者は、コンテンツ発行者自身、あるいはその代理人である。

【0077】2. 本発明適用のコンテンツ

本実施形態では、ハードウェア機構を利用してコンテンツが複製されないように保持するシステムにおいて、そのハードウェアが不正解析・改変され、コンテンツが複製された場合に、そのことを後から検出し、不正が行われたハードウェアを特定するようになっている。

【0078】但し、本実施形態において取り扱う不正は、コンテンツの複製のみであり、複製以外のコンテンツの改変などは対象としない。したがって、ハードウェアを解析、改変して可能となる不正が、コンテンツの複製のみであるか、あるいはコンテンツの複製のみが損害や影響の点で重要な場合に有効である。

【0079】さらに、取り扱われるコンテンツが正常に流通している場合には、唯一性があることを仮定する。つまり、このとき同一のコンテンツが存在すれば、ハードウェアの解析・改変によって不正なコンテンツの複製が行われたことになる。そのため、各コンテンツには改竄ができないように固有番号TIDが付けられているとする。そして、各装置間でのコンテンツ受け渡しの度に、コンテンツの固有番号TIDを含めて改竄がないことを検査できるようにする。これを以下では「コンテンツ確認」と呼ぶことにする。

【0080】コンテンツ確認ができる場合としては、例えば、コンテンツに固有の番号TIDと電子署名が付加されているコンテンツ構成が考えられる。図3には、コンテンツの構成例を示している。同図では、コンテンツには、コンテンツを特定する番号TIDと、コンテンツ発行者の署名証明書Certと、電子署名CSGが含まれる。コンテンツ発行者の署名証明書Certは、管理センタCA70により発行され、(Inf<sub>o<sub>i</sub></sub>, P<sub>i</sub>, S<sub>G<sub>i</sub></sub>)で構成される。また、電子署名CSGは、コンテンツ全体(但し、CSG部分は0とする)に対するコンテンツ発行者の電子署名である。コンテンツ本体とTIDとCertとCSG部にあたる0値のビット連結をMとおくと、コンテンツ発行者の電子署名CSG(=S<sub>G<sub>i</sub></sub>(M))は、D(S<sub>i</sub>, h(M))で表される。コンテンツ発行者の署名証明書Certによって、電子署名C

SGを検証するための鍵が得られるものとする。

【0081】この場合、コンテンツの改竄がないことは、図4にフローチャートの形式で示された処理手順によって確認することができる。以下、このフローチャートに従って、コンテンツの確認処理について説明する。

【0082】まず、署名証明書Certがコンテンツ発行者の署名証明書になっているかを確認する(ステップS1)。

【0083】次いで、管理センタCA70の公開鍵P<sub>CA</sub>を用いて署名証明書Certの検証を行う(h(Inf<sub>o<sub>i</sub></sub>, P<sub>i</sub>)=E(P<sub>CA</sub>, S<sub>G<sub>i</sub></sub>))(ステップS2)。

【0084】そして、署名証明書Certからコンテンツ発行者の公開鍵P<sub>i</sub>を抽出して(ステップS3)、この公開鍵P<sub>i</sub>を用いて電子署名CSGを検証する(h(M)=E(P<sub>i</sub>, CSG))(ステップS4)。

【0085】図3及び図4に示す例では、コンテンツは、順次明け渡されるコンテンツ保持装置10上で、複製されないようにハードウェア機構で保護される。さらにコンテンツ確認の処理も、不正解析に対する耐久性をもつハードウェアで行われる。コンテンツ譲渡の度に、コンテンツ確認を行うことで、改竄のないコンテンツのみが流通することになる。

【0086】また、図5には、コンテンツ確認を行うことができる他のコンテンツ構成例を示している。同図に示す例では、各コンテンツは、複製や改竄がされないように保護されるコンテンツ秘密部と、対応するコンテンツ公開部の組からなる。

【0087】コンテンツ秘密部は、コンテンツ毎に異なる公開鍵暗号の秘密鍵CS<sub>IT</sub>と付加情報で構成され、対応する公開鍵CP<sub>IT</sub>を含んだコンテンツ公開部とともに流通する。コンテンツ秘密部は、ICカードなど特定のコンテンツ保持装置10内で外部アクセス不可能な状態で保管される。

【0088】コンテンツ公開部には、公開鍵CP<sub>IT</sub>、コンテンツを特定する番号TIDと、コンテンツ発行者の署名証明書Certと、電子署名CSGが含まれる。コンテンツ発行者の署名証明書Certは、管理センタCA70により発行され、(Inf<sub>o<sub>i</sub></sub>, P<sub>i</sub>, S<sub>G<sub>i</sub></sub>)で構成される。CSGはコンテンツ公開部全体(但し、CSG部分は0とする)に対するコンテンツ発行者の電子署名である。コンテンツ本体とTIDとCertとCSG部にあたる0値のビット連結をMとおくと、コンテンツ発行者の電子署名CSG(=S<sub>G<sub>i</sub></sub>(M))は、D(S<sub>i</sub>, h(M))で表される。コンテンツ発行者の署名証明書Certによって、CSGを検証するための鍵が得られるものとする。コンテンツ公開部は、例えばICカードの外に、外部の装置からアクセス可能な状態に置かれる。

【0089】なお、図5に示すような秘密部と公開部とからなるコンテンツ構成に関しては、本出願人に既に譲

渡されている特願2000-378261号明細書（「情報記録媒体、情報処理装置及び情報処理方法、プログラム記憶媒体、並びに情報処理システム」）にも開示されている。

【0090】異なる公開鍵 $C_{PI0}$ を含むコンテンツ公開部に対応する秘密鍵 $C_{S10}$ を改竄することは、暗号学的に困難である。また、任意の公開鍵を含むコンテンツ公開部を新たに作成することは、コンテンツ公開部に含まれるコンテンツ発行者の電子署名 $C_{SG}$ によって困難である。これらの帰結として、ハードウェアの解析・改竄によって可能になる不正は、付加情報を改竄することか、保持しているコンテンツのコンテンツ秘密部を複製することである。付加情報は、チケットに対するはきみの役割をするため、その改竄によって可能となるのはチケットの不正な再利用である。本発明の目的は、複製による不正コンテンツの流通を阻止することなので、付加情報の改竄による不正は本明細書中では扱わない。以上から、特願2000-378261号明細書に開示される「情報記録媒体、情報処理装置及び情報処理方法、プログラム記憶媒体、並びに情報処理システム」の場合も、本発明の適用条件に合う。

【0091】図5に示したコンテンツに対して改竄がないことは、図6にフローチャートの形式で示した処理手順によって確認することができる。以下、このフローチャートに従って、コンテンツ確認処理について説明する。

【0092】まず、コンテンツ公開部の確認を行う。すなわち、コンテンツ公開部に含まれる署名証明書 $C_{ert}$ がコンテンツ発行者の署名証明書になっているかを確認し（ステップS11）、次いで、管理センターCA70の公開鍵 $P_{CA}$ を用いて署名証明書 $C_{ert}$ の検証を行う（ $h(\text{info}_0, P_1) = E(P_{CA}, SG_1)$ ）（ステップS12）。

【0093】次いで、署名証明書 $C_{ert}$ からコンテンツ発行者の公開鍵 $P_1$ を抽出して（ステップS13）、この公開鍵 $P_1$ を用いて電子署名 $C_{SG}$ を検証する（ $h(M) = E(P_1, CSG)$ ）（ステップS14）。

【0094】ステップS11～S14では、コンテンツ公開部の正当性を確認した。次いで、ステップS15以降では、コンテンツ秘密部側の正当性の確認を行う。本実施形態では、確認したコンテンツ公開部から公開鍵 $C_{PI0}$ を取り出し、これを使って対応するコンテンツ秘密部（秘密鍵 $C_{S10}$ ）が存在するかをチャレンジ・レスポンス認証によってコンテンツ秘密部の正当性を確認する。

【0095】チャレンジ・レスポンス認証では、まず、コンテンツ公開部が乱数 $r$ を生成するとともに、この乱数 $r$ を公開鍵 $C_{PI0}$ で暗号化したデータ $C$ をコンテンツ秘密部に送信する（ステップS15）。

【0096】コンテンツ秘密部側では、自身が持つコン

テンツ秘密鍵 $C_{S10}$ を用いて暗号データ $C$ を復号化して（ステップS16）、この復号結果 $R$ をコンテンツ公開部に返す（ステップS17）。

【0097】コンテンツ公開部は、コンテンツ秘密部から戻された値 $R$ と乱数 $r$ を比較して、認証を行う（ステップS18）。

【0098】図5及び図6に示す例では、コンテンツ保持装置10は、このコンテンツを複製されないためには、少なくともコンテンツ秘密部のみをハードウェア機構を利用して保護し、さらに、コンテンツ確認のうち少なくともコンテンツ秘密部を用いてレスポンス値を計算する手順については不正解析に耐久性のあるハードウェア上で行うようにする。コンテンツ保持装置間でコンテンツ譲渡を行う度に、上述したようなコンテンツ確認を行うことで、改竄のないコンテンツのみが流通することを保証することができる。

【0099】本実施形態ではさらに、コンテンツに一定の期限があり、ある一定期間の後にその大部分が回収されると想定する。ここで言う「回収」とは、コンテンツの発行者あるいはその代理人であるコンテンツ回収者の元にコンテンツが集められることを意味する。この回収は、コンテンツの有効期限による方法、例えばコンテンツが電子チケットである場合のように、特定日時に有効でその際に回収する方法などが考えられる。例えば改札に相当するコンテンツ回収装置50においてコンテンツの回収が行われる。

【0100】3. コンテンツ保持装置

本発明を適用するコンテンツ保持装置10としては、ここでは以下の説明を簡単にするために、コンテンツの保持装置全体がハードウェア的に耐久性があるICカードの場合を例にとって説明する。ICカードは、解析が困難なように設計・制作されており、通常はカード内部に保持されている情報を読み出すことができない。

【0101】図7には、本発明に適用可能なコンテンツ保持装置10の構成を模式的に示している。図7に示すように、コンテンツ保持装置10は、コンテンツ送受信部11と、メモリ部12と、認証処理部13と、電子署名秘部14と、暗号処理部15と、電子署名生成部16と、固有情報保持部17とで構成される。

【0102】コンテンツ送受信部11は、他のコンテンツ保持装置10や、コンテンツ発行装置、コンテンツ回収装置との間で、コンテンツを譲渡又は譲受するための機器間データ通信を行う。コンテンツの授受は、所定の認証手続を経た後に行われるが、その詳細は後述に譲る。

【0103】メモリ部12は、電子チケットなどのコンテンツや、乱数、譲渡履歴（後述）などの機器間認証処理に使用される作業データなどを保持する。

【0104】暗号処理部15は、共通鍵暗号アルゴリズム（前述）を用いた暗号化・復号化の処理を行う。



【0105】認証処理部13は、コンテンツを授受する相手（他のコンテンツ保持装置10や、コンテンツ発行装置30、コンテンツ回収装置50など）が正しくシステムに属する装置であるかを確認するための機能を持つ。この認証処理には、各装置が生成する電子署名や、管理センタ（CA）70による署名証明書を利用することができる。

【0106】固有情報保持部17は、コンテンツ保持装置10の署名証明書（ $Info_k$ ,  $P_k$ ,  $SG_k$ ）と、この証明書に含まれる公開鍵 $P_k$ に対応する秘密鍵 $S_k$ 、並びに、管理センタCA70の公開鍵 $P_{ca}$ 、コンテンツ保持装置10の固有番号 $HID_k$ などの認証処理に使用される固有情報が保持される。

【0107】電子署名生成部16は、自身の秘密鍵 $S_k$ を用いて自分の電子署名を生成する機能を持つ。データMが存在するとき、電子署名生成部16は自分の秘密鍵 $S_k$ を用いて、電子署名 $SG(M) = D(S_k, h(M))$ を計算する。データMを送る際に（M,  $SG(M)$ ）の組で送る（前述）。

【0108】また、電子署名検証部14は、他のコンテンツ保持装置10、コンテンツ発行装置30、コンテンツ回収装置50、並びに、管理センタCA70の電子署名を検証する機能を持つ。電子署名検証部14は、 $h(M) = E(P_k, SG(M))$ が満たされるかどうかを確認すること、Mが改竄されていないこと、電子署名 $SG(M)$ が秘密鍵 $S_k$ の所有者によって付加されたものであることを確認する（前述）。

【0109】勿論、本発明を実現する上で、コンテンツ保持装置10はICカードのみに限定されるものではない。例えば、特開平11-328850号公報に開示された情報配信システムや、特開2000-378261号明細書に開示された電子チケット・システムを、本実施形態に係るコンテンツ保持装置10として想定することも可能である。

【0110】4. コンテンツ発行装置  
本実施形態で言う「コンテンツ」は、例えば、乗車券、入場券、会員所、許可書、サービス券などに関する電子チケットを意味する。したがって、本実施形態に係るコンテンツ発行装置30は、電子チケットとしてのコンテンツを最初に生成する装置である。

【0111】コンテンツ発行装置30は、コンテンツ発行者に相当し、コンテンツとして保持されるべき情報を入力として受け付けて、これらの情報をコンテンツとして一時保持し、さらにコンテンツ保持装置10にコンテンツを譲渡する機能を持つ。但し、コンテンツを譲受した10は回収する機能は持たない。

【0112】図8には、本発明に適用可能なコンテンツ発行装置30の構成を模式的に示している。同図に示すように、コンテンツ発行装置30は、コンテンツ送受信部31と、メモリ部32と、認証処理部33と、電子署名

名検証部34と、暗号処理部35と、電子署名生成部36と、固有情報保持部37と、コンテンツ生成部38で構成される。

【0113】コンテンツ生成部38は、コンテンツとして保持されるべき情報を入力として受け付けて、電子チケットなどに相当するコンテンツを生成する。コンテンツとして保持されるべき情報としては、例えば、コンテンツ固有の識別情報TIDや、コンテンツ発行者による電子署名CSG、管理センタCA70から取得したコンテンツ発行者の署名証明書などである。生成されたコンテンツは、例えば、図3又は図5に示すデータ構造を持つ。

【0114】コンテンツ送信部31は、コンテンツ保持装置10に対してコンテンツを譲渡するための機器間データ通信を行う。ここで言うコンテンツの譲渡は、電子チケットなどに相当するコンテンツの販売に相当する。

【0115】メモリ部32は、電子チケットなどのコンテンツや、乱数、譲渡履歴（後述）などの機器間認証処理に使用される作業データなどを保持する。

【0116】暗号処理部35は、共通鍵暗号アルゴリズム（前述）を用いた暗号化、復号化の処理を行う。

【0117】認証処理部33は、コンテンツを授受する相手であるコンテンツ保持装置10が正しくシステムに属する装置であるかを確認するための機能を持つ。認証処理には、各装置が生成する電子署名や、管理センタ（CA）70による署名証明書を利用する。

【0118】固有情報保持部37は、コンテンツ発行装置30の署名証明書（ $Info_i$ ,  $P_i$ ,  $SG_i$ ）と、この証明書に含まれる公開鍵 $P_i$ に対応する秘密鍵 $S_i$ 、並びに、管理センタCA70の公開鍵 $P_{ca}$ 、コンテンツ発行装置30の固有番号 $HID_i$ などの認証処理に使用される固有情報が保持される。

【0119】電子署名生成部36は、自身の秘密鍵 $S_i$ を用いて自分の電子署名を生成する機能を持つ。データMが存在するとき、電子署名生成部36は自分の秘密鍵 $S_i$ を用いて、電子署名 $SG(M) = D(S_i, h(M))$ を計算する。データMを送る際に（M,  $SG(M)$ ）の組で送る（前述）。

【0120】また、電子署名検証部34は、コンテンツ保持装置10や管理センタCA70の電子署名を検証する機能を持つ。電子署名検証部34は、 $h(M) = E(P_k, SG(M))$ が満たされるかどうかを確認すること、Mが改竄されていないこと、電子署名 $SG(M)$ が秘密鍵 $S_k$ の所有者によって付加されたものであることを確認する（前述）。

【0121】5. コンテンツ回収装置

本実施形態で言うコンテンツの回収とは、例えば、乗車券、入場券、会員所、許可書、サービス券などに関する電子チケットを所定の改札において回収することを意味する。また、本実施形態では、図1に示したように、複

数のコンテンツ保持装置10間でやり取りされたコンテンツを最後に回収する装置として、コンテンツ回収装置50を想定する。

【0122】コンテンツ回収装置50は、改札に相当し、受け取ったコンテンツの表示や検査する機能を持つ。さらに、回収したコンテンツに対して、後述する不正検出と特定を行う。コンテンツ回収装置50は、他の装置にコンテンツを譲渡する機能は持たない。コンテンツ回収者だけが所持する。

【0123】図9には、本発明に適用可能なコンテンツ回収装置50の構成を模式的に示している。同図に示すように、コンテンツ回収装置50は、コンテンツ受信部51と、メモリ部52と、認証処理部53と、電子署名検証部54と、暗号処理部55と、電子署名生成部56と、固有情報保持部57と、コンテンツ回収部58、不正検出部59で構成される。

【0124】コンテンツ受信部51は、コンテンツ保持装置10からコンテンツを譲受するための機器間データ通信を行う。ここで言うコンテンツの譲受は、電子チケットなどに相当するコンテンツの回収に相当する。回収したコンテンツは、コンテンツ回収部58に蓄積される。

【0125】メモリ部52は、電子チケットなどのコンテンツや、乱数、譲渡履歴(後述)などの機器間認証処理に使用される作業データなどを保持する。

【0126】暗号処理部55は、共通鍵暗号アルゴリズム(前述)を用いた暗号化・復号化の処理を行う。

【0127】認証処理部53は、コンテンツを譲受する相手であるコンテンツ保持装置10が正しくシステムに属する装置であることを確認するための機能を持つ。認証処理には、各装置が生成する電子署名や、管理センタ(CA)70による署名証明書を利用する。

【0128】固有情報保持部57は、コンテンツ発行装置30の署名証明書(Info<sub>3</sub>, P<sub>3</sub>, SG<sub>3</sub>)と、この証明書に含まれる公開鍵P<sub>3</sub>に対応する秘密鍵S<sub>3</sub>、並びに、管理センタCA70の公開鍵P<sub>CA</sub>、コンテンツ回収装置50の固有番号HID<sub>5</sub>などの認証処理に使用される固有情報が保持される。

【0129】電子署名生成部56は、自身の秘密鍵S<sub>5</sub>を用いて自分の電子署名を生成する機能を持つ。データMが存在するとき、電子署名生成部56は自分の秘密鍵S<sub>5</sub>を用いて、電子署名SG(M) = D(S<sub>5</sub>, h(M))を計算する。データMを送る際に(M, SG(M))の組で送る(前述)。

【0130】また、電子署名検証部54は、コンテンツ保持装置10や管理センタCA70の電子署名を検証する機能を持つ。電子署名検証部54は、h(M) = E(P<sub>k</sub>, SG(M))が満たされるかどうかを確認することで、Mが改竄されていないことと、電子署名SG(M)が秘密鍵S<sub>k</sub>の所有者によって付加されたもので

あることを確認する(前述)。

【0131】不正検出部59は、コンテンツ受信部51においてコンテンツ保持装置10から譲受し、コンテンツ回収部58に格納された回収コンテンツを検査して、複数のコンテンツ保持装置10間でコンテンツの譲受が繰り返される仮定で不正が行われなかったかを検証する機能を持つ。不正検出部59は、例えばコンテンツの譲渡履歴を解析することによって、コンテンツ流通過程において不正行為が行われたことを検出したり、さらに不正行為が行われたコンテンツ保持装置を特定することが可能である。但し、不正検出処理の詳細については後述に譲る。

【0132】6. コンテンツの譲渡手続 ― 譲渡履歴、なしの場合。

上述した各装置10、30、50間でコンテンツが移動することをコンテンツの「譲渡」と呼ぶ。本実施形態では、装置間でコンテンツが移動する場合、コンテンツは暗号化されてやり取りされる。さらに、コンテンツを、やり取りすべきでない装置以外に渡したり、受け取ったりすることを防ぐために、他の装置との接続時には相互認証が行われる。

【0133】コンテンツの譲渡側及び譲受側の装置間での認証は、例えば同じシステムに属することが同じ共通鍵Kを保持することで確認することができる。図10には、装置間で行う認証手続の処理手順を模式的に示している。同図中で、a, bは、認証の開始側装置(a)と受け側装置(b)のどちらで暗号化されたかを区別するために、あらかじめ決まっている数値である。また、システムに属するすべてのコンテンツ保持装置10で共有されている。また、r1aは、数値rとaのビット連結を意味する。また、コンテンツの譲渡側の装置はコンテンツ保持装置10又はコンテンツ発行装置30であり、コンテンツの譲受側の装置は他のコンテンツ保持装置10又はコンテンツ回収装置50である。

【0134】まず、認証の開始側の装置が乱数r1を発生して、認証の受け側の装置に転送する。

【0135】これに対し、受側の装置は、受信した乱数r1とあらかじめ定められた値bとをビット連結して、これを共通鍵Kで暗号化して、暗号文cr1 (= E(K, r1 || b))を生成する。受側の装置は、さらに乱数r2を生成して、暗号文cr1とともに開始側の装置に返信する。

【0136】開始側の装置は、受信した暗号文cr1を共通鍵で復号化して平文R1 (= D(K, cr1))を生成する。そして、R1とr1bと比較して、両者が一致したならば、受側の装置を認証成立とする。開始側の装置は、さらに、受信した乱数r2とあらかじめ定められた値a(aはbとは異なる)とをビット連結して、これを共通鍵Kで暗号化して、その暗号文cr2 (= E(K, r2 || a))を受側の装置に送信する。

【0137】受け側の装置は、受信した暗号文 $c_{r2}$ を共通鍵で復号化して平文 $R2 (=D(K, c_{r2}))$ を生成する。そして、 $R2$ と $r2_{1a}$ を比較して、両者が一致したならば、開始側の装置を認証立する。

【0138】図10に示したような認証を通過することができるのは、同一システム内で共有される共通鍵 $K$ を持っている装置に限られる。したがって、この共通鍵 $K$ を同一システムに属するコンテンツ保持装置10すなわちICカードだけが共有しているとするれば、上述した認証を経ることによって、お互い4回同一システムに属することを確認することができる。この手順のことを、以降の説明では「認証手続き」と呼ぶことにする。

【0139】上述したような認証手続きがコンテンツの譲渡側及び譲受側の装置間で成功裏に終了すると、譲渡側の装置は、メモリ部12内のコンテンツを暗号化して譲受側の装置に転送する。

【0140】図11には、認証手続きの後に、コンテンツの譲渡側及び譲受側の装置間で行うコンテンツの転送手順を模式的に示している。

【0141】まず、コンテンツ譲渡側の装置は、コンテンツの暗号化用の鍵として用いる乱数 $K_r$ を新たに生成する。そして、このコンテンツ暗号化鍵 $K_r$ をコンテンツ譲受側の装置と共有するために、暗号化鍵 $K_r$ をシステム内で共有される共通鍵 $K$ で暗号化した暗号文 $c_{kr} (=E(K, K_r))$ をコンテンツ譲受側の装置に転送する。

【0142】次いで、コンテンツ譲渡側の装置では、電子チケットなどの送るべきコンテンツ $C_n$ を共有された鍵 $K_r$ で暗号化して、その暗号文 $c_n$ をコンテンツ譲受側の装置に転送する。

【0143】これに対し、コンテンツ譲受側の装置では、受け取った暗号文 $c_n$ を共有された鍵 $K_r$ で復号化して、元のコンテンツ $C_n$ を得る。次いで、コンテンツ譲受側の装置は、このコンテンツ $C_n$ についてコンテンツ確認を行う。

【0144】コンテンツが図3に示すようなデータ構造を持つ場合には、そのコンテンツ確認は、図4にフローチャート形式で示した処理手順に従い、署名証明書 $C_{er}$ の確認、管理センタCA70の公開鍵 $P_{ca}$ を用いた署名証明書 $C_{er}$ の検証、署名証明書 $C_{er}$ から抽出したコンテンツ発行者の公開鍵 $P_i$ を用いた電子署名CSGの検証によって行われる（前述）。あるいは、コンテンツが図5に示すように秘密部と公開部とに分かれたデータ構造を持つ場合には、そのコンテンツ確認は、署名証明書 $C_{er}$ の確認、管理センタCA70の公開鍵 $P_{ca}$ を用いた署名証明書 $C_{er}$ の検証、署名証明書 $C_{er}$ から抽出したコンテンツ発行者の公開鍵 $P_i$ を用いた電子署名CSGの検証によってコンテンツ公開部の正当性を確認した後に、チャレンジ・レスポンス認証によってコンテンツ秘密部の正当性を確認することによ

って行われる（前述）。

【0145】コンテンツ譲受側の装置は、コンテンツ確認に成功すると、コンテンツの受け入れをコンテンツ譲渡側の装置に通知する。これに応答して、コンテンツ譲渡側の装置では、メモリ部12に格納されている元のコンテンツ $C_n$ を削除する。また、コンテンツ譲受側の装置では、復号化されたコンテンツ $C_n$ を自分のメモリ部12に追加する。

【0146】メモリ部12内のコンテンツを暗号化して転送することでコンテンツの移動を行う手順を、以下の説明では「コンテンツ転送」と呼ぶことにする。

【0147】なお、コンテンツの譲渡などのデータ転送には通信エラーへの対策が本来は必要であるが、この点は本発明の要旨とは直接関連しないので、本明細書では説明を省略する。

【0148】7. 譲渡履歴の構造

本実施形態では、コンテンツを複数の装置間で授受を繰り返す過程で不正の行われた装置を特定するために、各コンテンツにコンテンツ保持装置間でやり取りの履歴を記録する「譲渡履歴」をさらに用意する。

【0149】譲渡履歴とは、コンテンツの譲渡の履歴を記録した情報のことである。図12は譲渡履歴のデータ構造の一例を示している。図示の譲渡履歴は、コンテンツの固有番号であるTIDと、1回のコンテンツ譲渡手続きが行われる毎に1ずつ追加されるレコード（レコード1、レコード2、…）とで構成される。

【0150】最初のレコードすなわちレコード1は、コンテンツ発行装置10からコンテンツ保持装置10Aへコンテンツが譲渡されたという譲渡履歴を示す。同様に、 $n$ 番目のレコード（レコード $n$ ）は、 $(n-1)$ 番目のコンテンツ保持装置から $n$ 番目のコンテンツ保持装置へコンテンツが譲渡されたという譲渡履歴を示す。

【0151】 $n$ 番目のレコードすなわちレコード $n$ は、コンテンツ譲渡の際におけるコンテンツ譲渡側の装置の固有番号HIDであるSID $_n$  (Sender ID) と、コンテンツ譲受側の装置の固有番号RID $_n$  (Receiver ID) と、時刻や乱数などからなる1回限りの敷（ノンス）である $N_n$ と、コンテンツ譲渡履歴の装置が生成したデジタル署名であるTSG $_n$ とで構成される。

【0152】TSG $_n$ は、譲渡履歴の全体に対するデジタル署名である。つまり、TIDとレコード1からレコード $n$ までのすべて（但し、レコード $n$ のデジタル署名TSG $_n$ の部分は0とする）に対するデジタル署名とする。すなわち、TIDとレコード1からレコード $n$ までのすべて（TSG $_n$ の部分は0）をデータ $M_n$ とおくと、TSG $_n$ は $D(S_n, h(M_n))$ と表される（但し、 $S_n$ は $n$ 番目にコンテンツ譲渡を行うコンテンツ保持装置の秘密鍵とする）。

【0153】譲渡履歴は、コンテンツ自体と異なり、唯一性を保つ必要はない。したがって、コンテンツ自体と

は分けて、コンテンツ保持装置10のユーザが読み書きできる記憶領域に保持することが可能である。但し、ユーザが不用意に改変を行った場合には、後述するコンテンツ譲渡の手続きで譲渡履歴交換が成功しなくなるので、そのようなことが容易に行われないように保持されることが望ましい。

【0154】8、コンテンツの譲渡手続 — 譲渡履歴を使用した場合

譲渡履歴を使用しない場合のコンテンツの譲渡手続については既に説明したので、ここでは、譲渡履歴を使用した場合のコンテンツの譲渡手続について説明する。

【0155】コンテンツを交換する過程で譲渡履歴の検証や譲渡履歴の更新を行う譲渡履歴管理部18を備えている(図2を参照のこと)。また、コンテンツ発行装置30は、コンテンツの譲渡時に譲渡履歴を生成する譲渡履歴生成部39を備えている(図2を参照のこと)。また、コンテンツ回収装置50における不正検出部59は、譲渡履歴の各レコードを解析してコンテンツ流通過程における不正を検出する機能を備えている。

【0156】図22には、譲渡履歴を加えた場合における、コンテンツ保持装置間でのコンテンツ譲渡を行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、譲渡履歴を利用したコンテンツ譲渡手続について説明する。

【0157】譲渡履歴を加えた場合のコンテンツの移動においては、まず、コンテンツ保持装置間で認証手続を行う(ステップS51、S52)。装置間の認証手続については、既に図10を参照しながら説明したので、ここでは説明を省略する。

【0158】装置間での認証手続に成功した場合には、次いで、譲渡履歴の受け渡しを行なう譲渡履歴交換が行われる(ステップS53、S54)。但し、以下のデジタル署名認証から、コンテンツを交換する相手側の装置が同一システムに属することが確認できるとき、例えば署名証明書が同一のシステムに属するコンテンツ保持装置に対してのみ発行されている場合(すなわち、共通鍵Kを保持していることと同じ場合には、認証手続きに代えて、譲渡履歴交換を行えばよい、譲渡履歴の好手続の詳細については後述に譲る。

【0159】譲渡履歴の交換に成功した後は、上述のコンテンツ転送(図11を参照のこと)を行う(ステップS55、S56)。

【0160】そして、コンテンツの転送に成功した後に、譲渡された譲渡履歴とコンテンツの双方に含まれる固有番号TIDが一致することを確認して、コンテンツの譲渡が完了する(ステップS57)。

【0161】図13には、コンテンツの譲渡側と譲受側のコンテンツ保持装置間で行われる譲渡履歴の交換手続について模式的に示している。また、図14には、この

譲渡履歴の交換手続のうち、譲渡側のコンテンツ保持装置から譲受側のコンテンツ保持装置へのデジタル署名認証の処理手順を、フローチャートの形式で示している。

(譲受側のコンテンツ保持装置から譲渡側のコンテンツ保持装置へのデジタル署名認証の処理手順は、図14と同様であるので説明を省略する。)以下、図13及び図14を参照しながら、譲渡履歴の交換手続について説明する。

【0162】まずコンテンツ譲渡側の保持装置は、自分の署名証明書をコンテンツ譲受側の保持装置に送付する(ステップS21)。署名証明書としては、コンテンツ譲渡側の保持装置と結びつく情報 $Info_n$ と $P_n$ を組にしたもの( $Info_n$ ,  $P_n$ )に、管理センタCA70が自分の秘密鍵 $S_{CA}$ を使って生成した署名 $S_{G_n} = D(S_{CA}, h(Info_n, P_n))$ を付加した証明書(前述)を使用することができる。

【0163】これに対し、コンテンツ譲受側の保持装置では、署名証明書の検証を行う(ステップS22)。管理センタCA70の公開鍵 $P_{CA}$ を用いて証明書の署名認証を行うことによって( $h(Info_n, P_n) = E(P_{CA}, S_{G_n})$ )、証明書の正当性を検証することができる(前述)。

【0164】そして、証明書が正しい場合には、コンテンツ譲受側の保持装置は、乱数 $r$ を発生して(ステップS23)、この乱数 $r$ をコンテンツ譲渡側の保持装置に送る(ステップS24)。

【0165】コンテンツ譲渡側の保持装置では、受け取った乱数に署名 $Sgn = D(S_n, h(r))$ を生成して(ステップS25)、これをコンテンツ譲受側の保持装置に返送する(ステップS26)。

【0166】コンテンツ譲受側の保持装置では、電子署名 $Sgn$ が自ら発生した乱数 $r$ に対応するコンテンツ譲渡側の保持装置の署名として正しいかどうかを検証する(ステップS27)。署名の正当性は、コンテンツ譲渡側の保持装置の公開鍵 $P_n$ を用いて、 $h(r) = E(P_n, Sgn)$ によって検証することができる。

【0167】そして、上述と同様に、コンテンツ譲受側の保持装置からコンテンツ譲渡側の保持装置に対してもデジタル署名認証を行うことで、両コンテンツ保持装置はお互いの署名検証鍵とIDを正しく把握することができるようになる。コンテンツ譲受側の保持装置のIDは、レコードの作成時(後述)に用いられる。

【0168】次いで、コンテンツ譲受側の保持装置では、大きなビット数の乱数や時刻情報から、毎回(コンテンツを譲渡する度に)異なる数 $N$ のストリーム $TN_n$ を発生し、これをコンテンツ譲渡側の保持装置に送付する。

【0169】コンテンツ譲渡側の保持装置では、譲渡履歴を更新して、新規レコードを生成する。新規レコード $n$ は、コンテンツ譲渡の際におけるコンテンツ譲渡側の装置の固有番号SID $n$ と、コンテンツ譲受側の装置の

固有番号R ID<sub>0</sub>と、ノンスTN<sub>0</sub>とで構成される(前述)。

【0170】最後に、コンテンツ読取側の保持装置は自らの秘密鍵S<sub>0</sub>を使って、新規レコードを含む読取履歴全体に対する電子署名TSG<sub>0</sub>を生成し(但し、新規レコード中のTSG<sub>0</sub>部分を0として計算する)、新規レコードに追加する(前述)。更新された読取履歴は、コンテンツ読取側の保持装置に送付される。

【0171】これに対し、コンテンツ受信側の保持装置では、受信した読取履歴の確認を行う。すなわち、先行する電子署名の検証手続きを介して把握したコンテンツ読取側の保持装置のIDが新規レコードのSID<sub>0</sub>に、自分のIDがRID<sub>0</sub>に正しく含まれること、並びに、先に自身が発生したものと同一ノンスTN<sub>0</sub>が含まれることを確認する。そして最後に、コンテンツ読取側の保持装置の署名検証鍵P<sub>0</sub>を使って新規レコードの署名TSG<sub>0</sub>が正しく読取履歴に対するコンテンツ読取側の保持装置の署名になっていることを検証する。署名TSG<sub>0</sub>の検証は、TIDとレコード1からレコードnまでのすべて(TSG<sub>0</sub>の部分は0)をデータM<sub>0</sub>とおくと、h(M<sub>0</sub>)=D(P<sub>0</sub>, TSG<sub>0</sub>)によって行うことができる。

【0172】コンテンツ読取側の保持装置での読取履歴の確認が成功した場合には、コンテンツ読取側の保持装置では元の読取履歴を削除し、コンテンツ読取側の保持装置では受け取った読取履歴を保存して、読取履歴交換が終了する。

#### 【0173】9. 不正検出と特定

上述したコンテンツ読取手続き(図11を参照のこと)を行うことで、各コンテンツには、コンテンツの発行者(発行装置30)から現在のコンテンツ所有者(保持装置10)までの読取の履歴が記録された読取履歴(図12を参照のこと)が付属することになる。

【0174】各コンテンツは唯一性があり、同時には単一のコンテンツ保持装置(HIDで区別される)でのみ保持されている。各コンテンツ保持装置は装置の固有番号HIDによって識別可能であるので、固有番号TIDで識別される特定のコンテンツの読取履歴は一種類であるべきである。

【0175】ところが、ハードウェアの不正解析が行われコンテンツが複製された場合を想定すると、あるTIDを割り当てられたコンテンツが複数のコンテンツ保持装置上に同時に保持されるようになり、この結果、不正行為が行われたTIDに対して複数の読取履歴が生じる。

【0176】ここで、読取履歴が完全である場合、すなわちコンテンツ保持装置10の解析によりコンテンツの不正複製が行われたとしても、読取履歴は上述した手順で正しく記録される場合(読取履歴は改竄が不可能である場合)について考察してみる。

【0177】最初にコンテンツ発行者はコンテンツが唯一になるように発行するので、これらの読取履歴は不正を行ったコンテンツ保持装置に到達するまでは、唯一のコンテンツとともに単一の読取履歴のみに存在する。しかし、不正が行われたコンテンツ保持装置からの読取履歴に付随するレコードはそれぞれ異なり、以降は異なる読取履歴になる。以下では、これを読取履歴の「枝分かれ」と呼び、枝分かれの発生したレコードを「枝分かれレコード」と呼ぶことにする。読取履歴の枝分かれによって、不正が行われて複製されたコンテンツに対しては複数種類の読取履歴が生じる。

【0178】不正によってコンテンツが複製されると、有効期限切れや改札などコンテンツ回収装置50によるコンテンツ回収によって、特定のコンテンツ(すなわち、特定のTID)が複数回収されることになる。まず、単一のTIDが2回以上回収されたということから、コンテンツが読取される途中で不正が行われたことが判明する。

【0179】さらに、このコンテンツ複製による読取履歴の枝分かれに対応して、複数種類の読取履歴が回収されることになる。この回収された複数の読取履歴を解析して、枝分かれレコードを探索することで、そのレコードの送り側IDすなわちSIDのコンテンツ保持装置を不正に行われたコンテンツ保持装置として特定することができる。

【0180】以上の説明では、読取履歴の完全性が保たれていることを前提としている。しかしながら、本発明はこのような前提に拘束されるものではなく、この読取履歴がコンテンツの不正複製を行うようなコンテンツ保持装置でどのように改竄されても、不正を行ったコンテンツ保持装置を特定することができる。

【0181】以下では、不正には読取履歴を改竄することを含めて、不正を行なったコンテンツ保持装置を特定する場合について説明する。併せて、不正を行うコンテンツ保持装置が複数あり且つそれらが共謀する場合であっても、不正を行った複数のコンテンツ保持装置のうち少なくとも1つを特定できることを示す。

#### 【0182】10. 不正特定の假定

読取履歴の不正改竄や、複数のコンテンツ保持装置の共謀を検出する上で、以下の2点を仮定する。すなわち、

(1) 不正によって可能になるのは、自分あるいは仲間所有するコンテンツ保持装置に保持されているコンテンツの複製、及び、そのコンテンツ保持装置のデジタル署名の生成である。

(2) コンテンツの読取履歴を改竄できるのは、読取履歴が自分のコンテンツ保持装置内に保持されている期間だけである。すなわち、他人が保持している読取履歴は改竄できない。

【0183】これらの假定はコンテンツの読取履歴に基づく不正行為の検出を実装する上で現実的な条件である

ということ、当業者であれば容易に理解できるであろう。

【0184】11. 不正検出と不正者特定の手順  
コンテンツの読渡履歴を利用した不正検出、及び不正コンテンツ保持装置の特定は、以下に示す4段階の手順によって構成される。また、図15には、コンテンツの読渡履歴を利用して不正検出、及び不正コンテンツ保持装置を特定するための処理手順をフローチャートの形式で示している。以下、このフローチャートを参照しながら、不正検出と不正者特定の手順について説明する。

【0185】(1) 同一固有番号TIDを持つコンテンツが複数回回収されていないかどうかを検査する(ステップS31)。もし、TIDの異なるすべてのコンテンツが1回ずつしか回収されていないければ、不正は行われていないので、本処理手順を終了する。他方、同じTIDを持つコンテンツが2回以上回収された場合には、その読渡履歴を集めて、TID毎に手順(2)以降の処理を行う。

【0186】(2) TIDが同じそれぞれの読渡履歴について、含まれるすべてのレコードについて新しいものから古いものに辿りながら電子署名TS<sub>G</sub>を検証する(ステップS34～S37)。途中電子署名が正しくないレコードkが見つかった場合、その次のレコードk+1の送り側(つまり検証できないレコードを受け入れた装置)で不正が行われたことになる(ステップS43)。手順(2)で不整合が見つからない読渡履歴については、次の手順(3)に進む。

【0187】(3) TIDが同じそれぞれの読渡履歴について、読渡履歴の先頭レコード(すなわち最も古いレコード)のコンテンツ読渡側となった装置(SID)が、当該コンテンツすなわちチケットの発行者(HID<sub>ISSUER</sub>)が否かを判断する(ステップS38)。先頭レコードのコンテンツ読渡側となった装置(SID)がチケットの発行者(HID<sub>ISSUER</sub>)でない場合、このコンテンツ読渡側の装置が不正を行ったコンテンツ保持装置の番号になる(ステップS44)。そうでない読渡履歴、すなわち単体の読渡履歴からは不正が特定できないものについては、一旦フールしておく(ステップS39)。その上で、処理中のTIDで他に未処理の読渡履歴があれば、そちらについても上記の手順(2)及び(3)を実行する(ステップS40)。同一のTIDを持つすべての読渡履歴について処理が終わったならば、次の手順(4)に進む。

【0188】(4) フールされている同一TIDの読渡履歴が複数存在する場合には、互いの読渡履歴を比較して、それらの枝分かれレコードを探す。枝分かれレコードにおけるコンテンツ読渡側のコンテンツ保持装置(SID)が不正を行ったことになる(ステップS41)。

【0189】12. 不正者を特定できることの証明  
ここで、上記の「11. 不正検出と不正者特定の手順」

によって不正者を特定することができること、すなわち、不正を行っていない者が誤って不正者に特定されることがないことを証明しておく。

【0190】上述した手順(1)は、不正の検出である。

【0191】また、上述した手順(2)では、読渡履歴に含まれるレコードに不整合がある場合、その不整合から改竄を行った者を特定する。以下、この特定手順が成功することを、コンテンツ保持装置が正しく動作し、上記コンテンツ読渡手順が正しく行われる限り、誤って不正が行われたコンテンツ保持装置と特定されないことを示し、その対偶として証明する。

【0192】あるコンテンツ保持装置(HID<sub>n-1</sub>)から別のコンテンツ保持装置(HID<sub>n</sub>)にコンテンツすなわち電子チケットが読渡される際に追加されたレコードnには、HID<sub>n-1</sub>の電子署名が付加されている(前述)。手順(3)により、コンテンツ保持装置HID<sub>n</sub>はこの電子署名を検証し、整合性がない場合には受け取りを拒否するはずである。したがって、仮定(2)、並びに、コンテンツ保持装置HID<sub>n</sub>が正しく動作するという前提条件により、正しいレコードnが追加された読渡履歴が次のコンテンツ保持装置HID<sub>n+1</sub>に渡される。ある1つのコンテンツ保持装置HID<sub>n</sub>に注目したとき、それが上述した手順(2)で不正とみなされるのは、新しいレコードから遡っていったときに、コンテンツ保持装置HID<sub>n</sub>の受け入れたレコードnではじめて不整合になるときである。しかし、以後のチケット保持者が不正を行わない限り、レコードnの電子署名が不整合になることはない。

【0193】次に、HID<sub>n</sub>より後に読渡を受けるコンテンツ保持装置が不正を行う場合、例えば、固有番号HID<sub>p</sub>(p>n)を持つコンテンツ保持装置が、以前のどれかのレコードを改変した場合を考え、これによって、レコードnより以降に追加されたレコードの電子署名の整合性を保ちながら、レコードnの電子署名の整合性が失われるような改変の可能性について考察してみる。

【0194】レコードpにはHID<sub>p-1</sub>の電子署名が付加されており、その電子署名はレコードpを含む読渡履歴全体に対するものである。したがって、あるレコードk(k<p)の改変により、レコードkの電子署名だけでなく、レコードkとレコードpの間のすべてのレコードの電子署名が不整合になる。

【0195】HID<sub>p</sub>がこの部分のレコードの不整合をすべて解消できるのは、仮定(1)により、それらのレコードに電子署名したコンテンツ保持装置がすべて自分あるいは仲間のみ所有である場合に限られる。前提条件から、コンテンツ保持装置HID<sub>n</sub>は正しく動作するので、レコードn+1に含まれるコンテンツ保持装置HID<sub>n</sub>の電子署名の整合性を取ることはできない。したが

って、レコードkとレコードpの間にレコードnが含まれる場合、レコードnを不整合とし、レコードn+1以降が整合性を保つような改変を行うことはできないことが分かる。

【0196】上述した手順(3)では、談話履歴の各レコードに関して整合性が保たれるような改変について扱う。上述した通り、コンテンツ保持装置H1D<sub>3</sub>が過去のレコードkを改変した場合、レコードkからレコードpまでのすべてのレコードが不整合となる。仮定(1)より、コンテンツ保持装置H1D<sub>3</sub>はこのうち過去に自分又は共謀者が生成した履歴レコードのみに整合性を持たせることができる。このため、コンテンツ保持装置H1D<sub>3</sub>にできることは、こうした履歴レコードR<sub>q</sub>を改変してそれ以降の整合性の取れない履歴レコードを捨て去るか、又は、既存の履歴レコードをすべて捨て去ってコンテンツ保持装置H1D<sub>3</sub>が談話履歴の最初のレコードを作成することである。前者の場合は検出できない。後者の場合は、先頭レコードが送り側の装置がコンテンツすなわち電子チャットの発行者の電子署名と異なることから検出可能である。

【0197】これまでの議論をまとめると、過去に不正者あるいはその共謀者が生成した履歴レコードを改変し、それ以降のレコードを削除した場合、あるいは談話履歴の改変を行わなかった場合以外は、談話履歴自体の整合性の検査から、不正が検出されることが分かる。

【0198】したがって、コンテンツ保持装置H1D<sub>3</sub>でコンテンツの複製を行った不正者が、談話履歴自体の整合性の検査で特定されることを避けた場合、通常のコンテンツ談話をレコードp+1を加えるか、又は、過去に不正者あるいはその共謀者が生成した履歴レコードR<sub>q</sub>を改変してR<sub>q</sub>とし、R<sub>q</sub>以降の談話履歴レコードを削除することである。

【0199】上述した手順(4)により、これらの場合が取り扱われる。何故なら、どちらの場合でも、談話履歴に不正者又はその共謀者の番号がコンテンツ談話側となるレコードが含まれ、上記のコンテンツ談話をあわせて2回以上行くと、枝分かれレコードとして検出することが可能になる。不正者が同じ相手に談話する場合でも、その相手も不正を行っていない限り、この談話に対するレコード中のノンスが各回で一致しないため、枝分かれレコードとして検出される。

【0200】以上から、不正検出と不正者特定の手順(1)～(4)によって、不正の検出と不正者特定ができることが示された。

【0201】1.3. 談話履歴の暗号化

ここでは、コンテンツ流通の匿名性についてもう一度取り扱う。

【0202】既に述べたように、各装置の所有者とコンテンツ保持装置の固有番号であるH1D<sub>3</sub>との対応は、管理センタC A70だけが把握していることによ

り、管理センタC A70以外の通常の利用者に対しては、コンテンツ流通の匿名性が守られる。

【0203】しかしながら、場合によっては特定の保持装置(特定個人と対応すること等価)で、どのようなコンテンツが保持されていたかの記録を収集することが重要な情報となる。また、何らかの方法によって装置の固有番号H1D<sub>3</sub>と利用者の対応関係が特定された場合、談話履歴はある特定個人がどのようなコンテンツを好むかといったことを知るための手がかりとなってしまう。コンテンツ利用者のプライバシーが侵害されるおそれがある。

【0204】このような場合に対処するために、管理センタC A70とコンテンツ談話の当事者以外は談話履歴を参照できなくする方法について、以下に説明する。そのためにまず、管理センタC A70は公開鍵暗号の公開鍵及び秘密鍵のペアを生成する。ここでは、管理センタC A70の公開鍵をP<sub>CA</sub>とし、その秘密鍵をS<sub>CA</sub>とする。管理センタC A70は公開鍵P<sub>CA</sub>だけを公開する。そして、利用者はこの公開鍵P<sub>CA</sub>を使って談話履歴を暗号化することで、管理センタC A70のみが談話履歴を参照できるようにする。

【0205】公開鍵P<sub>CA</sub>は、例えば、コンテンツ中に改変されないように含ませればよい。図16には図3に示した構成のコンテンツ中に公開鍵P<sub>CA</sub>を含ませた様子を示し、また、図17には図5に示した構成のコンテンツ中の公開鍵P<sub>CA</sub>を含まれた様子を示している。また、談話履歴は、図18に示すように、コンテンツの識別番号T1D以外のすべてのレコードがP<sub>CA</sub>を用いて暗号化された状態で流通する。

【0206】図19には、このように談話履歴を暗号化した場合のコンテンツ談話の手順を模式的に示している。この場合、図13を参照しながら既に説明した「談話履歴あり」の場合のコンテンツ談話手順と同様の処理手順を踏めばよい。但し、談話履歴更新において、コンテンツ談話側のコンテンツ保持装置によって生成された新規レコードに含まれる電子署名は、以前の談話に対応する暗号化されたレコードを含んだ談話履歴全体に対するものとする。談話履歴は、追加された新規レコードが暗号化されないまでコンテンツ談話側のコンテンツ保持装置に渡す。

【0207】コンテンツ談話側のコンテンツ保持装置では、談話履歴の確認において、新規レコードに含まれる電子署名を検証する。そして、検証が成功して終了した後に、新規レコードを管理センタC A70の公開鍵P<sub>CA</sub>を用いて暗号化して、談話履歴の最後尾の暗号化されていない新規レコードをそれと置換する。

【0208】次いで、不正検出と不正者特定について説明する。但し、不正者は、コンテンツの複製を行なった者、談話履歴の改変を行なった者、並びに、管理センタC A70の公開鍵P<sub>CA</sub>を用いて談話履歴レコードを正し

く暗号化しなかった者とする。

【0209】不正検出と不正者特定の手順は、既に説明した手順と同様でよい。但し、手順(2)において読取履歴に含まれるレコードを検証する際に、管理センタCA70の秘密鍵 $S_{CA}$ を用いて各レコードを復号化する作業が加わる。この秘密鍵 $S_{CA}$ によって正しく復号化できること、及び、レコード中の電子署名が正しいことによつて各レコードの正当性が証明される。

【0210】レコードが正しくない場合、すなわちレコードが正しく復号できないか又は電子署名が正しくない場合には、そのレコードを読受した側のコンテンツ保持装置、すなわち、当該レコードの次のレコードを送ったコンテンツ保持装置が不正を行ったことを示している。これ以外の点に関しては、読取履歴を暗号化しない場合と同様であるので、説明を省略する。

【0211】このように、読取履歴の各レコードを管理センタCA70の公開鍵 $P_{CA}$ で暗号化した場合、読取履歴を所定のシステム管理者以外には読めないようにすることができる。この結果、システム管理者には不正が行われたコンテンツ保持装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどのコンテンツ保持装置を経由してきたかを秘密にすることができる。

【0212】「追補」以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。例えば、本発明を実現する上で、特定の暗号アルゴリズムに限定されるものではない。要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0213】

【発明の効果】以上詳記したように、本発明によれば、デジタル情報を耐久性のあるハードウェア上に保持することによって、複数の機器間でデジタル情報の読取を繰り返す過程において不正利用から保護することができる。優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0214】また、本発明によれば、デジタル情報を複数の機器間で読取を繰り返す過程において、万一ある機器ハードウェアが解析・改変された場合であってもデジタル情報を不正利用から保護することができる。優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0215】また、本発明によれば、ハードウェアの解析・改変によるデジタル情報の不正利用を検出することによってハードウェアの解析・改変への潜在的な意図を抑制することができる。優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0216】本発明によれば、ハードウェアの耐タンパ性を用いて情報コンテンツの複製や改変を防ぐ機能を実現している装置において、ハードウェアの不正解析が行われてコンテンツの複製並びに他の装置に読取された場合であっても、それらのコンテンツを回収して検査することで、不正の発生を検出し、さらに不正が行われた装置を特定することができる。

【0217】本発明においてコンテンツの読取履歴を検査する機能を実現するために、装置間でのコンテンツのやり取りの度にコンテンツ複製の有無を確認する必要がない。また、装置間でのコンテンツのやり取りの度にコンテンツ複製の有無を確認する必要がないので、コンテンツ授受の際にオンラインの確認などが必要なく、不正検出のために必要な計算量負荷やメモリ容量を軽減することができる。

【0218】不正者がハードウェアの解析・改変の結果として、コンテンツの複製によって利益を得ようとしても、本発明によれば不正なコンテンツ保持装置が特定されその装置の所有者として不正者が特定あるいは絞り込めることから、不正者がハードウェア解析・改変を行う意図を抑制するという効果がある。また、不正者の特定を可能としながら、コンテンツの利用者の匿名性、すなわち誰がどのようなコンテンツを利用したかといったプライバシー情報を守ることができる。

【図面の簡単な説明】

【図1】本発明を適用する対象となる、デジタル情報すなわちコンテンツを複製されないように保持するシステム1の構成を模式的に示した図である。

【図2】コンテンツ保持装置10、コンテンツ発行装置30、コンテンツ回収装置50に対して管理センタ(CA)70が電子署名の証明書を発行する仕組みを模式的に示した図である。

【図3】コンテンツの構成例を示した図である。

【図4】図3に示したコンテンツの改竄がないことを確認するための処理手順を示したフローチャートである。

【図5】コンテンツ確認を行うことができる他のコンテンツ構成例を示した図である。

【図6】図5に示したコンテンツの改竄がないことを確認するための処理手順を示したフローチャートである。

【図7】本発明に適用可能なコンテンツ保持装置10の構成を模式的に示した機能ブロック図である。

【図8】本発明に適用可能なコンテンツ発行装置30の構成を模式的に示した機能ブロック図である。

【図9】本発明に適用可能なコンテンツ回収装置50の構成を模式的に示した機能ブロック図である。

【図10】コンテンツの読取履歴及び読受側の装置間で行う認証手続(但し、読取履歴を用いない場合)の処理手順を説明するための図である。

【図11】コンテンツの読取履歴及び読受側の装置間で認証手続を経た後に各装置間で行うコンテンツの転送手続



を説明するための図である。

【図12】 譲渡履歴のデータ構造の一例を示した図である。

【図13】 コンテンツの譲渡側と譲受側のコンテンツ保持装置間で行われる譲渡履歴の交換手順を模式的に示した図である。

【図14】 譲渡側のコンテンツ保持装置から譲受側のコンテンツ保持装置へのデジタル署名認証の処理手順を示したフローチャートである。

【図15】 コンテンツの譲渡履歴を利用して不正検出、及び不正コンテンツ保持装置を特定するための処理手順を示したフローチャートである。

【図16】 図3に示した構成のコンテンツ中に公開鍵P<sub>CA</sub>を含ませた様子を示した図である。

【図17】 図5に示した構成のコンテンツ中に公開鍵P<sub>CA</sub>を含ませた様子を示した図である。

【図18】 コンテンツの識別番号TID以外のすべてのレコードがP<sub>CA</sub>を用いて暗号化された状態を示した図である。

【図19】 譲渡履歴を暗号化した場合のコンテンツ譲渡の手順を模式的に示した図である。

【図20】 譲渡履歴の受け渡しを伴うコンテンツの移動を行うタイプのコンテンツ保持装置10の構成を模式的に示したブロック図である。

【図21】 譲渡履歴の受け渡しを伴うコンテンツの移動

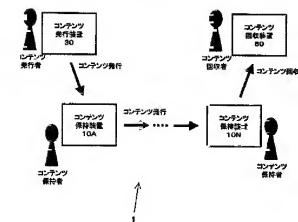
を行うタイプのコンテンツ発行装置30の構成を模式的に示したブロック図である。

【図22】 譲渡履歴を加えた場合にコンテンツ保持装置間でコンテンツを交換するための処理手順を示したフローチャートである。

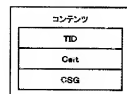
【符号の説明】

- 10…コンテンツ保持装置
- 11…コンテンツ送受信部、12…メモリ部
- 13…認証処理部、14…電子署名検証部
- 15…暗号処理部、16…電子署名生成部
- 17…固有情報保持部
- 18…譲渡履歴管理部
- 30…コンテンツ発行装置
- 31…コンテンツ送信部、32…メモリ部
- 33…認証処理部、34…電子署名検証部
- 35…暗号処理部、36…電子署名生成部
- 37…固有情報保持部、38…コンテンツ生成部
- 39…譲渡履歴生成部
- 50…コンテンツ回収装置
- 51…コンテンツ受信部、52…メモリ部
- 53…認証処理部、54…電子署名検証部
- 55…暗号処理部、56…電子署名生成部
- 57…固有情報保持部、58…コンテンツ回収部
- 59…不正検出部
- 70…管理センタ(CA)

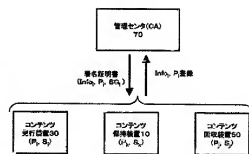
【図1】



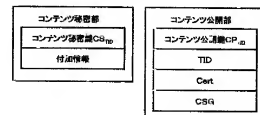
【図3】



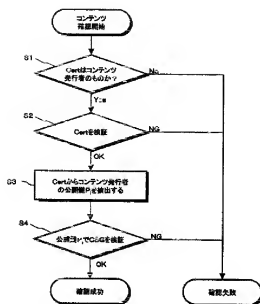
【図2】



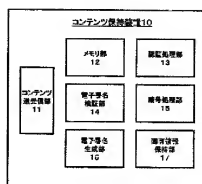
【図5】



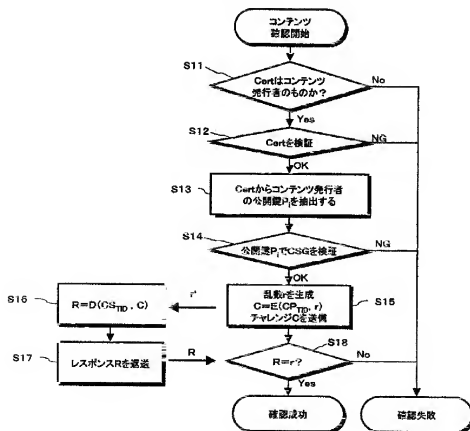
【図4】



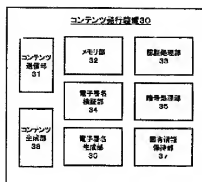
【図7】



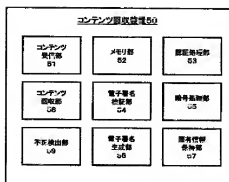
【図6】



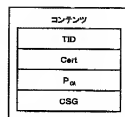
【図8】



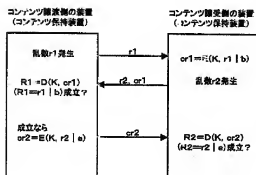
【図9】



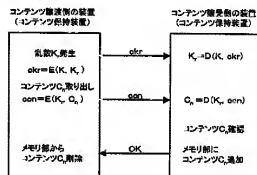
【図16】



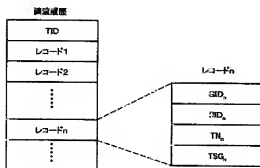
【図10】



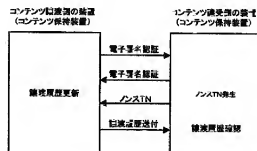
【図11】



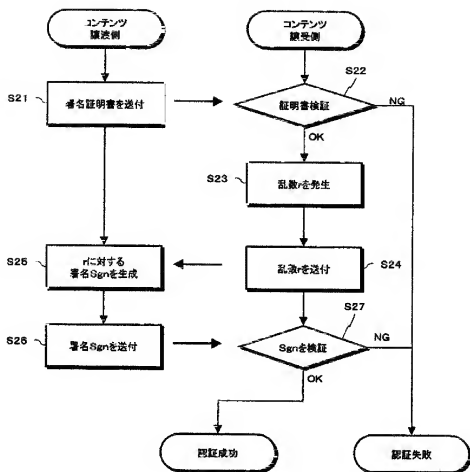
【図12】



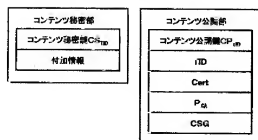
【図13】



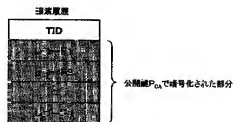
【図14】



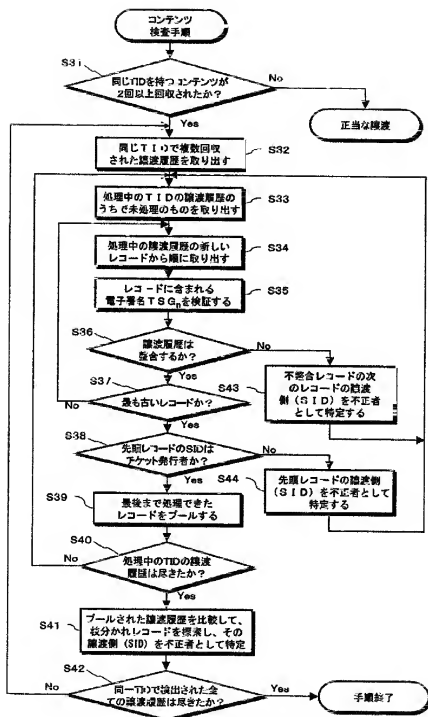
【図17】



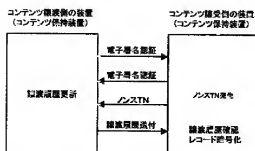
【図18】



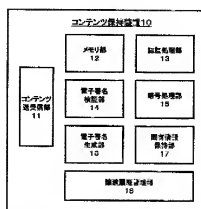
【図15】



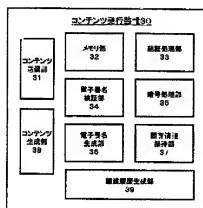
【図19】



【図20】



【図21】



【図22】

